

Version Version 3.5
Part No. 312538-A Rev 01
December 2000

600 Technology Park Drive
Billerica, MA 01821-4130

Managing the Contivity Stateful Firewall

NORTEL
NETWORKS™

Copyright © 2000 Nortel Networks

All rights reserved. December 2000.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Bay Networks, Nortel Networks Extranet Switch, and Contivity are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY

COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks NA Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface	13
Before you begin	13
Text conventions	14
Related publications	15
Hard-copy technical manuals	15
How to get help	16
 Chapter 1	
Introducing the Firewall	17
Firewall concepts	17
Component descriptions	18
Stateful inspection	18
Interfaces	19
Filter rules	20
NAT	20
Anti-spoofing	21
Attack detection rules	21
Firewall options	21
 Chapter 2	
Configuring the Firewall	23
Licensing	23
Prerequisites	24
Installing Java 2 software	25
Using Internet Explorer	25
Using Netscape	26
Using Netscape 6	28
Using Netscape on Solaris	28
Initial Configuration	29
Contivity Firewall options	32
Setting up policies on the firewall	32
Creating and editing firewall policies	33

Navigating rules	34
Implied rules	35
Override rules	36
Interface-specific rules	36
Default rules	38
Post-implied rules	39
Performing actions on rules	39
Header row menu	40
Row menu	40
Cell menus	41
Rule columns	42
Creating policies	49
Adding a policy	49
Deleting an existing policy	50
Copying an existing policy	50
Renaming an existing policy	51
Creating a new policy example	51
Verifying your configuration	55

Chapter 3

Configuring Interface NAT..... 57

Network Address Translation (NAT)	57
Translation types	57
Interface NAT	60
Enabling interface NAT policies	60

Chapter 4

Monitoring the Firewall..... 67

Logging	67
SNMP traps	69
Reports	70

Chapter 5

Command Line Interface..... 71

Accessing the CLI	71
-------------------------	----

Access from a telnet session	71
Access from the Serial Port menu	72
Command modes	73
Key bindings	75
Commands	76
firewall	76
firewall anti-spoof / tunnel filter / connection number	78
firewall logging	80
license	82
netobj	84
netobj-group	86
policy nat	88
policy nat interface	90
policy security	92
rule (Firewall Policy Configuration)	94
rule (NAT Policy Configuration)	97
service	99
service-group	101
show firewall	103
show interfaces	105
show license	107
show netobjs	109
show policy nat	111
show policy security	113
show rules (Firewall Policy Configuration)	115
show rules (NAT Policy Configuration)	117
show services	119
Appendix A	
Error Messages	121
Firewall messages	121
Index	125

Figures

Figure 1	Implied rules	35
Figure 2	Override rules	36
Figure 3	Interface-specific rules	37
Figure 4	Source interface rules	38
Figure 5	Destination interface rules	38
Figure 6	Default rules	39
Figure 7	Post-implied rules	39
Figure 8	Header row menu	40
Figure 9	Row menu	40
Figure 10	Cell menu (option)	41
Figure 11	Cell menu (procedure)	41
Figure 12	Rule column	42
Figure 13	Rule column for interface-specific rules	43
Figure 14	Tunnel dialog box for a user tunnel	43
Figure 15	Tunnel Selection dialog box for a branch office tunnel	44
Figure 16	Network Object Selection dialog box	45
Figure 17	network object edit dialog box	45
Figure 18	Service Object Selection dialog box	46
Figure 19	tcp object insert dialog box	47
Figure 20	Action column options	47
Figure 21	Log column options	48
Figure 22	Status column options	48
Figure 23	Firewall - Select Policy screen	49
Figure 24	Static address translation	58
Figure 25	Port address translation	59
Figure 26	Pooled address translation	60
Figure 27	Serial Port menu	72

Tables

Table 1 CLI Modes, Prompts, and Access 74

Table 2 Nortel Networks CLI (NNCLI) key bindings 75

Preface

This guide introduces you to the Nortel Networks™ Contivity® Stateful Firewall. Topics include:

- Firewall concepts
- Configuring the firewall
- Monitoring the firewall
- Firewall command line interface

Complete details for configuring and monitoring the Contivity VPN Switch are in *Configuring the Contivity VPN Switch* and the *Reference for the Contivity VPN Switch*.

Before you begin

This guide is intended for network managers who are responsible for setting up the software for the Contivity VPN Switch and the Contivity Stateful Firewall. This guide assumes that you have the following background:

- Experience with windowing systems or graphical user interfaces (GUIs)
- Familiarity with the network management

Text conventions

This guide uses the following text conventions:

braces ({})

Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.

Example: If the command syntax is

show ip {alerts|routes}, you must enter either **show ip alerts** or **show ip routes**, but not both.

brackets ([])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.

Example: If the command syntax is

show ip interfaces [-alerts], you can enter either **show ip interfaces** or **show ip interfaces -alerts**.

italic text

Indicates file and directory names, new terms, book titles, Web addresses, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.

Example: If the command syntax is

show at <valid_route>, *valid_route* is one variable and you substitute one value for it.

plain Courier
text

Indicates command syntax and system output, for example, prompts and system messages.

Example: Set Trap Monitor Filters

arrow (→)	Shows menu paths. Example: Protocols→IP identifies the IP option on the Protocols menu.
vertical line ()	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is show ip {alerts routes} , you enter either show ip alerts or show ip routes , but not both.

Related publications

For more information about using the Contivity Stateful Firewall, refer to the following publications:

- Release notes provide the latest information, including known problems, workarounds, and special considerations.
- *Configuring the Contivity VPN Switch* provides complete details on configuring, monitoring, and troubleshooting your switch.
- *Reference for the Contivity VPN Switch* provides details on the Contivity VPN switch user interface screens.

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the support.baynetworks.com/library/tpubs/ Web address. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems Web address at www.adobe.com to download a free copy of Acrobat Reader.

You can purchase selected documentation sets, CDs, and technical publications though the Internet at the www1.fatbrain.com/documentation/nortel/ Web address.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Billerica, MA	800-2LANWAN or (800) 252-6926
Santa Clara, CA	800-2LANWAN or (800) 252-6926
Valbonne, France	(33) (4) 92-96-69-68
Sydney, Australia	(61) (2) 9927-8800
Tokyo, Japan	(8) (3) 5740-1700

Chapter 1

Introducing the Firewall

This chapter introduces the Contivity Stateful Firewall and provides an overview of the firewall components.

Firewall concepts

The Contivity Stateful Firewall provides a secure access point between an internal network and an external network, such as the Internet. The firewall allows you to protect your network and the information on it from unauthorized intrusion from external networks. The firewall provides a line of defense to allow acceptable traffic, as defined by your organization, and to drop all unacceptable traffic before it enters or leaves the network. It monitors packets and sessions to make decisions based on established rules to determine the appropriate actions to take.

By using *stateful inspection*, the Contivity Stateful Firewall provides a high level of security, the fastest runtime, and the flexibility to define the rules to fit your environment. The firewall delivers full firewall capabilities, assuring the highest level of network security. To do this, the firewall examines both incoming and outgoing packets running against a common security policy. All service rules are interpreted on IP conversations (not packets) and are fully stateful. Service rules do not filter packets directly, but the firewall services determine how to process them based on the security policy defined. The firewall provides a user interface to help you determine the appropriate rules for your network.

The Contivity Stateful Firewall achieves optimum performance as a result of advanced memory management techniques and optimized packet inspection.

In addition, you can configure the firewall to log some or all significant events. This includes all connections over the network, such as all e-mail transactions, firewall status changes, and system failures. You can use the logged information to help enhance network security or track unauthorized use.

Component descriptions

The following sections provide brief descriptions of the various components of the firewall.

Stateful inspection

Some protocols are difficult to allow through a firewall securely using traditional filtering mechanisms. In FTP, for example, where the control connection is typically created using a known port, but the data connection is over a random port. To allow an FTP data connection through a firewall without leaving a large number of open ports requires stateful inspection: packets are inspected at the application layer to determine which port the data connection is using. Traffic on that port can then be allowed to pass through the firewall for the duration of the FTP session.

Transport-level state inspection provides a number of ways to make TCP traffic more secure and more difficult for hackers to intercept. Stateful inspection of TCP consists of verifying the consistency of the TCP header as well as preventing some well-known TCP attacks. TCP sequence numbers are randomized to prevent sequence number guessing.

Stateful inspection of an application is unique for each application. Any non-predicted ports used by an application are validated and allowed through the firewall using stateful inspection. The following applications are inspected:

- FTP
- TFTP
- RCMD
- SQLNET
- VDOLive
- RealAudio

A *conversation* is created for all unique end-to-end communication. For instance, an FTP session between a client and a server can consist of several streams of traffic, with both data and control packets flowing back and forth. All of this traffic is contained in the same conversation. Since the Contivity Stateful Firewall also supports tunneled traffic, each unique tunnel (end user or branch office) would be identified by its own conversation.

Interfaces

The Contivity VPN Switch has many interfaces. Each tunnel (end user or branch office) is a virtual interface, and all switches have two or more physical interfaces. Packets can be classified by the interface on which they arrive at the switch (the source interface) or the interface on which they leave the switch (the destination interface).

The rules in a policy can be constructed to either use or ignore this classification. If the rule designates “Any” as an interface, the rule ignores this classification. If the rule designates any other name as the interface, the rule uses this classification.

The rules in any policy can use the following terms to designate an interface:

- Any – Any physical interface or tunnel.
- Trusted – Any private physical interface or tunnel.
- Untrusted – Any public physical interface.
- Tunnel:Any – Any tunnel, excluding any physical interfaces.
- For tunnels that are also interfaces, you can specify either a group name for user tunnels or the specific branch office tunnel for branch office tunnels.
- Tunnel:/base – For tunnels that are also interfaces, you can specify the specific branch office tunnel. For example, /base/mktng/tony refers to branch office tony in group /base/mktng.
- Tunnel:user – For tunnels that are also interfaces, you can specify a group name for user tunnels. For example, /base/engineering refers to all user tunnels in that group.
- Interface name – The value of the Description field assigned to the physical interface on the System→LAN (or System→WAN) screen. If the description is blank, the interface name defaults to the value of the Interface field on the same screen.

Any physical interface can be marked as “Private” or “Public” on the System→LAN→Configure screen. By default, the LAN interface (Slot 0) is “Private” and all other interfaces are “Public.”

Filter rules

Filtering uses a set of rules to determine whether a packet should be allowed through the firewall. Typical options are either accept or drop the packet, which provides a degree of security for a network. The rules determine one of the following actions:

- Accept the packet
- Drop the packet
- Reject the packet by sending a reject to the source address
- Log the packet locally, which is a modifier for the previous three actions

For further explanation of the rules and how they are applied, see “Navigating rules” in Chapter 2.

NAT

Network Address Translation (NAT) is the translation of one network IP address that is used within a LAN to a different IP address that is used outside the LAN. This feature allows a system to be identified by one address on its own network, yet be identified by a totally different address to systems on a different network.

NAT helps you avoid any issues with diminishing IP address space by allowing multiple systems on the same network to share the same IP address. It also provides additional security by minimizing the number of private network addresses that are visible to the public network. For tunneled traffic, it allows multiple intranets with conflicting subnets to communicate. For physical traffic, it provides support for dynamic as well as static NAT.

Applying NAT to traffic patterns is independent of whether the source or destination of the packet is private or public. The following traffic patterns are equivalent:

- Private to private

- Private to public
- Public to private
- Public to public

Anti-spoofing

Anti-spoofing is a method used to prevent a packet from forging its source IP address. Typically, the source address of each packet is examined and validated. Anti-spoofing performs the following checks:

- That the source address is not equal to the destination address
- That the source address is not equal to zero

Attack detection rules

When a common attack is launched against corporate networks, the firewall should be able to detect these attacks. It should also drop any packets resulting from the attack, preventing denial-of-service as well as non-authorized intruders. The Contivity Stateful Firewall provides defense against well-known Denial of Service attacks with well-known prevention methods.

Firewall options

You can select one of the following firewall options:

- Contivity Firewall
- Check Point FireWall-1
- No Firewall

The Contivity Firewall consists of the Contivity Stateful Firewall, Contivity Interface Filter, Contivity Tunnel Filter, Interface NAT, and anti-spoofing. (In previous releases, the Contivity Interface Filter was called the Contivity Firewall.) You can enable or disable each of these separately. However, you must enable either the Contivity Stateful Firewall or Contivity Interface Filter.

The Check Point Firewall-1 requires that you have Check Point FireWall-1 Management Console Software and the appropriate license. For further information, see *Installing Check Point FireWall-1 on the Contivity Extranet Switch*.

The No Firewall option disables all firewall features on the switch. In this configuration, the switch performs VPN routing only.

Chapter 2

Configuring the Firewall

This chapter describes the steps for setting up your firewall. The process consists of the following:

- Firewall software installation process
- Firewall configuration tasks on the Contivity VPN Switch
- Configuration tasks on the firewall
- Steps you can use to verify that your firewall is working properly

The procedures assume that you have already configured your Contivity VPN Switch (except for the firewall component) and that you have obtained the required firewall license. To configure the switch, see *Configuring the Contivity VPN Switch*.

Licensing

The Admin→Install keys menu item is used to install a licensing key that enables optional software functionality. In order to enable features, a license key must first be installed.

To install a software license key:

- 1** Go to the Admin→Install Keys screen.
- 2** Type the key that you obtained from Nortel Networks Customer Support in the box to the right of Firewall.
- 3** Click on the Install button.

After a valid key is installed, the label “Key Installed” is displayed. It is only necessary to install a key once on each switch.

You must remove the firewall license key if you are downgrading the switch to a release earlier than Version 3.5. Click on the Remove button to remove the key. A confirmation message appears and when you click on Yes, the key is removed.

Prerequisites

Before you start setting up your firewall, be sure you have the management IP address of your switch. This address is found on the switch's System→Identity screen. You may also need the following information:

- The name of the firewall, which is the name that is used by the Domain Name Service (DNS) server to identify the management address of the switch. This name is entered in the DNS Host Name field of the switch's System→Identity screen.
- The names and IP addresses of your switch's interfaces. These are found on the switch's Status→Statistics: Interfaces screen.

System requirements necessary to access the Contivity Stateful Firewall Manager include:

- Supported operating systems and platforms include Solaris (OS 2.6, 7, or 8) on a x86 or SPARC platform and Microsoft® Windows 95, 98, 2000, or Windows NT 4.
- Required software includes Java 2 Plug-in V1.3.0, available in the Java 2 Runtime Environment V1.3.0. The J2RE is available for automatic download on a Windows platform from the switch (refer to the Java 2 Runtime Environment Installation). J2RE installation files for Windows and Solaris are also available on the Nortel Networks CD in the tools/java directory.
- Supported browsers include Internet Explorer 4 and higher and Netscape Navigator/Communicator 4 and higher. Netscape 6 currently comes with a version of the Java 2 Plug-in that is not supported. If you wish to use Netscape 6, please refer to the Netscape section of the Java 2 Runtime Environment Installation.

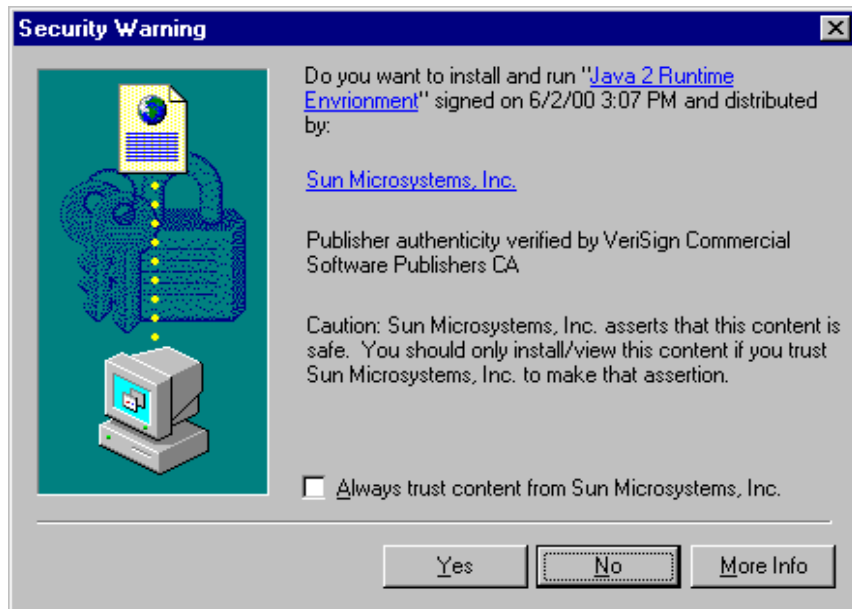
Installing Java 2 software

To access the Contivity Stateful Firewall Manager, the computer used to administer you switch must have the Java 2 Runtime Environment installed. There are two separate procedures that you can use to install the Java 2 software, depending on whether you use Internet Explorer or Netscape Navigator to access the switch.

Using Internet Explorer

To install the Java 2 software on Windows 9x, Windows 2000, or Windows NT from Internet Explorer:

- 1 Connect to the management IP address of the switch and log in.
- 2 Go to the Services→Firewall screen.
- 3 Click on the Manage Policies button. A popup window appears and tries to load the Contivity Stateful Firewall Manager.
- 4 When the Security Warning dialog box appears, click on Yes to install the Java 2 Runtime Environment.



The installation program will begin to download the software from the switch. This may take several minutes to load, depending on the speed of your connection to the switch.

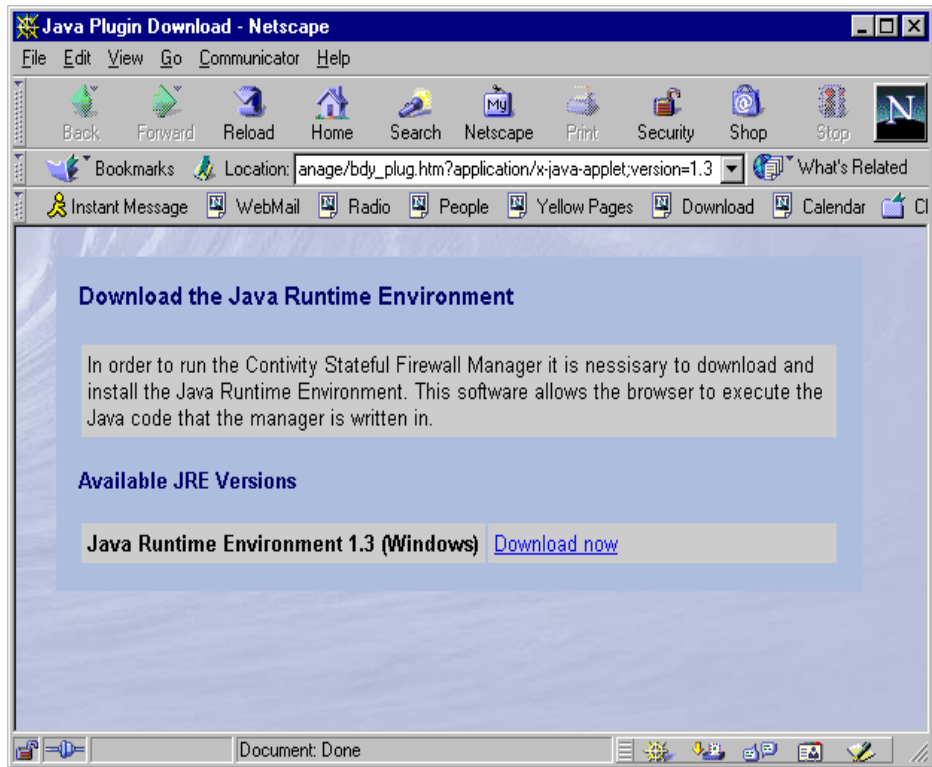
- 5 When the installation program displays the Software Licensing Agreement, click on Yes to accept the agreement.
- 6 When the installation program asks for an installation location, accept the default location or choose an alternate installation location.
- 7 Click on Next > to finish the installation.
- 8 When the installation is complete, close all open Web browsers.
- 9 Reboot the computer for the changes to take effect.

Using Netscape

To install the Java 2 software on Windows 9x, Windows 2000, or Windows NT from Netscape Navigator:

- 1 Connect to the management IP address of the switch and log in.
- 2 Navigate to the Services→Firewall screen.
- 3 Click on the Manage Policies button. A popup window appears and tries to load the Contivity Stateful Firewall Manager. The Plug-in Not Loaded dialog box appears. (If this dialog does not appear, click on the long white or gray box that appears on the browser popup window.)

- 4 Click on the Get the Plug-in button to download the Java 2 Runtime Environment. The Java Plugin Download screen appears.



- 5 Click on the Download now link next to the Windows version of the Java Runtime Environment.
- 6 When the browser prompts you for a location to save the file, choose a download location and click on OK to continue. (This may take several minutes to load, depending on the speed of your connection to the switch.)
- 7 When the download finishes, go to the download location and double-click on the icon for the Java Runtime Environment.
- 8 When the installation program displays the Software Licensing Agreement, click on Yes to accept the agreement.
- 9 When the installation program asks for an installation location, accept the default location or choose an alternate installation location.
- 10 Click on Next > to finish the installation.

- 11 When the installation is complete, close all open Web browsers.
- 12 Reboot the computer for the changes to take effect.

Using Netscape 6

Netscape 6 currently includes a version of the Java 2 Plug-in that is not supported (version 1.3.01). To successfully load the Contivity Stateful Firewall Manager, you must use version 1.3.0. The following steps change the default plug-in from version 1.3.01 to version 1.3.0.

- 1 Install the Java 2 Runtime Environment 1.3.0 as described above and be sure to restart the computer.
- 2 Load the Java Plug-in Properties from Start>Settings>Control Panel>Java Plug-in.
- 3 Click on the Advanced tab.
- 4 Choose JRE 1.3.0 ... from the list.
- 5 Click on Apply.
- 6 Close the window.
- 7 Close all open instances of Netscape.
- 8 Restart Netscape. The correct plug-in should be available.

Using Netscape on Solaris

The Java 2 Runtime Environment for Solaris is available on the Nortel Networks CD. The installation files and instructions are available for x86 and SPARC platforms.

To install the Java 2 software on Solaris (OS 2.6, 7, 8) from Netscape Navigator:

- 1 Ensure that a version of Netscape is installed on the computer.
- 2 Close all instances of Netscape if any are opened.
- 3 Go to the tools/java/solaris directory on the Nortel Networks CD.
- 4 Choose the subdirectory for the installed platform, either intel for x86 or sparc for SPARC.
- 5 Copy the binary (.bin) and the README files to the computer.

- 6 Follow the platform-specific installation instructions contained in the README file.
- 7 Set the `NPX_PLUGIN_PATH` environment variable to the directory containing the `javaplugin.so` file.

For example, if the J2RE was installed in the `/usr/j2re1.3` directory, the command to set the `NPX_PLUGIN_PATH` from the C shell, it would be `setenv NPX_PLUGIN_PATH "/usr/j2re1.3/plugin/sparc` on a SPARC platform." From the C shell, it would be `setenv NPX_PLUGIN_PATH "usr/j2re1.3/plugin/i386` on a x86 platform."

- 8 Start Netscape and then close it.
- 9 Start Netscape again and the plug-in should be available.

Initial Configuration

To use the firewall on the Contivity VPN Switch, you must first enable the firewall service. Without the firewall enabled, the switch only handles traffic on the tunnel interfaces. When the firewall is enabled, the switch can also handle IP traffic between the physical interfaces and the tunnel interfaces.

You must create rules for tunnel traffic before traffic on existing tunnel definitions is allowed. The Contivity Stateful Firewall uses the principle that whatever traffic is not specifically allowed is disallowed. The rule set of the active policy is applied to all traffic, including tunneled and non-tunneled traffic. Therefore, when the Contivity Stateful Firewall is first enabled, all traffic is disallowed until you configure rules specifically allowing certain types of traffic.

To get started using the firewall, follow these steps:

- 1 Go to the System→LAN screen. For each interface, click on Configure and enter a one-word label in the Description field. You use this name to identify interfaces in the security policy rules. LAN represents the physical port interface to which you assign an IP address. Slot *n* Interface *n* represents an optional LAN card in expansion Slot *n* using Interface *n*.

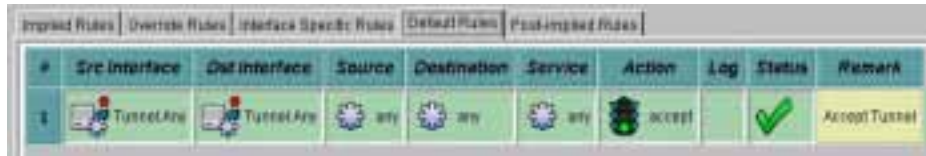
For example, you could make Internet the description for Slot 1 Interface 1 and ServiceNet the description for Slot 2 Interface 1. The description is case sensitive and cannot be abbreviated when specifying the interface in the rules. If you do not specify a description, the default name for the interface is “Slot n Interface 1” ($n=1$ to 4) is case sensitive, and cannot be abbreviated.

- 2 Go to the Services→Firewall/NAT screen.



- 3 Check the boxes next to Contivity Firewall, Contivity Stateful Firewall, NAT, and Anti-spoofing.
- 4 Click on OK. A confirmation screen appears asking if you want to reboot.
- 5 Click on Later.
- 6 Return to the Services→Firewall/NAT screen.
- 7 Click on the Edit button next to the Contivity Firewall. Again a screen appears asking if you want to reboot.
- 8 Click on OK. You **must** reboot the switch. On subsequent screens, confirm that the switch must be rebooted.
- 9 After the switch reboots, return to the Services→Firewall/NAT screen.

- 10 Click on Manage policies to load the Contivity Stateful Firewall Manager applet. The first time you do this on any workstation, you need to load the Java applet. You see the message “Retrieving policies.”
- 11 Select the System Default policy, which is read-only.
- 12 Click on the View button to review this policy. The implied and post-implied rules are included with every new policy.



#	Src Interface	Dst Interface	Source	Destination	Service	Action	Log	Status	Remark
1	TunnelAny	TunnelAny	any	any	any	accept		✓	Accept Tunnel

- 13 To exit the Contivity Stateful Firewall Manager, click on Manager→Exit. You can toggle the browser windows between the Contivity Stateful Firewall Manager applet and the Services→Firewall/NAT screen. If you use your browser to change other settings on the switch while the Contivity Stateful Firewall Manager applet is running, these changes are not reflected in the current Contivity Stateful Firewall Manager applet. Click on the Firewall icon in the Contivity Stateful Firewall Manager applet to refresh the list of policies and other switch settings. Any changes made in the Contivity Stateful Firewall Manager applet are not evident in the Services→Firewall/NAT screen until you save a policy.
- 14 After you exit the Contivity Stateful Firewall Manager applet, click on Refresh on the Services→Firewall/NAT screen.

You can apply (assign) a policy to the firewall in either the Contivity Stateful Firewall Manager applet or the Services→Firewall/NAT screen. The new policies you create are not automatically applied to the firewall. Only one policy at a time can be in effect on the firewall.



Note: You cannot import or import new policies. However, there are no restrictions on creating new policies.

Contivity Firewall options

The following options control the amount of detail recorded in the event log. None of these options apply to the system log.

- All – includes Traffic, Policy Manager, Firewall, and NAT
- Traffic – logs when flows and conversations are created or removed
- Policy Manager – logs firewall processes and when rules and policies are created
- Firewall – logs how the firewall handles packets within a flow
- NAT – logs NAT-related events
- Debug – creates special log messages intended for use only by Nortel Networks customer support

You can also select a connection number, which allows you to reserve memory for a maximum number of connections. Determining the optimum memory allocation makes it easier to tune your system for firewall traffic. Under the Connection Number section, type in any connection number. Below the box for the connection number is a suggested number range. The range displayed varies depending on the model and amount of memory for your switch. Each IPSec tunnel requires two connections. Setting the connection number to the minimum number in the number range minimizes the number of IPSec tunnels that your switch can handle and maximizes the size of dynamic memory available to the other firewall processes. Nortel Networks recommends that you set the number near the middle of the range displayed unless you have specific requirements that you need to consider.

Setting up policies on the firewall

Firewall service consists of two primary components: the *service properties* and the *security policy*. The properties that define what service is being offered include a service name, the protocol (TCP, UDP, ICMP), and the port number (or range) on which the server listens.

Security policies consist of a set of rules that specify what traffic is allowed or denied. You can define custom policies when more complex security policies are needed and the standard policies are not sufficient. By customizing your policies, you can further refine the control over what traffic is allowed on your internal networks.

The firewall policies use standard actions, which represent the most commonly used policies. You can use the following actions individually or combine them in a single rule:

- Allow (accept) access if traffic arrives on a specified interface (source interface rule)
- Allow access if traffic from the firewall is to a specified interface (destination interface rule)
- Allow access if traffic is from a specific host or group of hosts
- Allow access if traffic is going to a specific host or group of hosts
- Allow access if traffic is a specific service
- Deny access (drop) or deny access and send a reject packet (reject) if specified as modifiers to the previous actions

A set of rules defines a specific security policy. A rule defines whether communication should be accepted or rejected (or logged) based on its source, destination, and service.

You must create rules for tunnel traffic before traffic on existing tunnel definitions will be allowed. The Contivity Stateful Firewall uses the principle that whatever traffic is not specifically allowed is disallowed. The rule set of the active policy is applied to all traffic, including tunneled and non-tunneled traffic. Therefore, when the Contivity Stateful Firewall is first enabled, all traffic is disallowed until you configure rules specifically allowing certain types of traffic.

Creating and editing firewall policies

Access control parameters are implemented through the graphical user interface or the command line interface (CLI). Using either interface, you can configure the following:

- Network objects
- Service objects

- Rules

See Chapter 5, “Command Line Interface” for a list of commands you can use on the CLI.

The security policy is a set of rules describing the required behavior of the service. You specify all rule fields for service policies using service objects. Each rule consists of a combination of network objects, services, actions, and logging mechanisms.

Navigating rules

The firewall policy edit screen allows you to add, delete, and modify the rules in a policy. This screen is divided into the following rule groups:

- Implied rules
- Override rules
- Interface-specific rules
- Default rules
- Post-implied rules

Rules are divided into the following types:

- *Implied* rules are processed first by the firewall. These rules permit tunnel termination and access to the management interface. They are derived from the Services→Available screen settings.
- *Override* rules are the first set of rules specified in the policy. These rules allow you to quickly override the rest of the rules in the policy, possibly for a short period while debugging a problem. These rules do not specify a specific interface in the source or destination interface column. You may only select from the interface groupings (Any, Trusted, Untrusted, Tunnel:Any).
- *Interface-specific* rules are rules that apply only to packets that enter or leave the switch through one specific interface (physical or tunnel). The interface-specific section is divided into two types: source rules and destination rules. Source rules are those rules that define the selected interface as their source and destination rules are those rules that define the selected interface as their destination. The interface names correspond to the names that you configured on either the System→LAN or System→WAN screen on

your switch. On these screens, you can also specify whether these interfaces are private or public. For tunnels that are also interfaces, you can specify either a group name for user tunnels or the specific branch office tunnel for branch office tunnels.

- A *default* rule set is applied to all packets for which a rule was not found in the set of interface-specific rules. These rules cannot specify specific interfaces in the source or destination interface columns and can only use interface groupings (Any, Trusted, Untrusted, Tunnel:Any).
- *Post-implied* rules allow RSVP, ICMP, LDAP and RADIUS access and access by routing protocols on trusted interfaces. You cannot configure these rules and the last post-implied rule is to drop all traffic that was not handled by a prior rule. However, you can override these rules by specifying a rule in one of the three rule groupings (override, interface-specific, or default).

Implied rules

The implied (Figure 1) rules are rules that are defined by the system. You cannot modify them using the Contivity Stateful Firewall Manager. These rules are read-only and you cannot modify any part of the rule. They are generated from the Services→Available screen on the switch. These sections are for display purposes only.

Figure 1 Implied rules

#	Src Interface	Dest Interface	Source	Destination	Service	Action	Log	Status	Remark
1	Private	Any	any	_SystemIP	http https ftp telnet	accept		☒	
2	Any	Private	_SystemIP	any	any	accept		☒	

Override rules

Rules that are specified in the override rules (Figure 2) are the first set of rules specified in the policy. The purpose of these rules is to allow you to quickly override the rest of the rules in the policy, possibly for a short period while debugging a problem. These rules do not specify a specific interface in the source or destination interface column. You can only select from the interface groupings (Any, Trusted, Untrusted, Tunnel:Any).

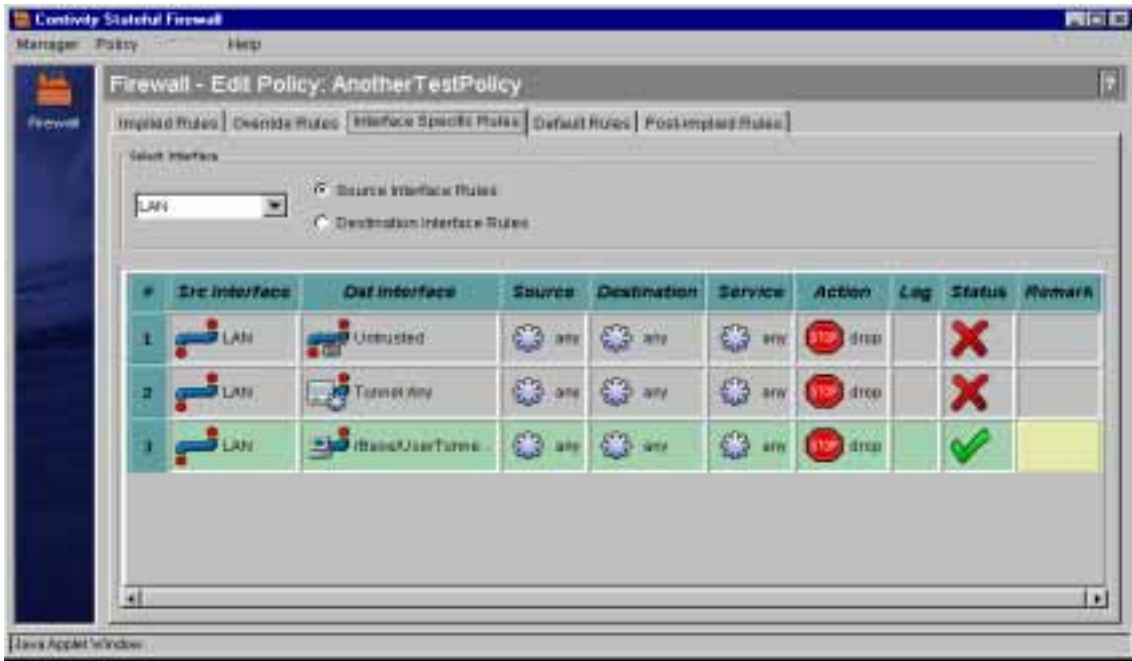
Figure 2 Override rules



Impaled Rules Override Rules Interface Specific Rules Default Rules Post-implier Rules									
#	Src Interface	Dest Interface	Source	Destination	Service	Action	Log	Status	Remark
1	 Any	 Any	 Any	 Any	 smtp	 drop	☒		

Interface-specific rules

Interface-specific rules are rules that only apply to one specific interface (physical or tunnel). The interface-specific rule section (Figure 3) has a selection box that allows you to select the interface to display rules. The interface-specific rule section only displays one interface at a time. In order to view all of the interface-specific rules, select All Interfaces. This screen has a column that denotes which rules are source and destination rules.

Figure 3 Interface-specific rules

Selecting an interface from the selection box displays those rules that apply to the selected interface. If you select Branch Office Tunnel or User Tunnel from the primary selection box, a new selection box appears next to it that contains the branch office tunnels or user groups. This box disappears if you later select a physical tunnel.

The interface-specific section is also divided into two types: source rules and destination rules. Source rules are those rules that define the selected interface as their source and destination rules are those rules that define the selected interface as their destination. You can toggle between the two types of rules for a particular interface by clicking on the Source Rules or Destination Rules radio button.

When you add a rule to the interface-specific section, the rule is created as the same type as the one you are currently viewing.

If you are viewing the source rules (Figure 4) and you add a new rule from that screen, it is a source rule. The source interface field on a source rule is set to the current interface and is read-only. The destination interface field can contain any physical interface, tunnel, or interface grouping.

If you are viewing the destination rules (Figure 5) and you add a new rule from that screen, it is a destination rule. The destination interface field on a destination rule is set to the current interface and is read-only. The source interface field can only contain interface groupings (Any, Trusted, Untrusted, Tunnel:Any).

Figure 4 Source interface rules



Figure 5 Destination interface rules



Default rules

A default rule (Figure 6) is a rule that is applied to all packets for which a rule was not found in the set of interface-specific rules. These rules cannot specify specific interfaces in the source or destination interface columns and can only use interface groupings (Any, Trusted, Untrusted, Tunnel:Any).

Figure 6 Default rules



Post-implied rules

The post-implied (Figure 1) rules are rules that are defined by the system. You cannot modify them using the Contivity Stateful Firewall Manager. These rules are read-only and you cannot modify any part of the rule. They are generated from the Services→Available screen on the switch. These sections are for display purposes only.

Figure 7 Post-implied rules



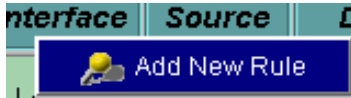
Performing actions on rules

The actions that you can perform on rules are controlled by menus that you access by right-clicking on an option. Each of these menus controls a different aspect of the rule.

Header row menu

Right-clicking on any of the header cells brings up the Header row menu (Figure 8). This menu contains one item, Add New Rule. This menu item allows you to add a new rule to the top of the list. The new rule appears in position one and all existing rules increment by one.

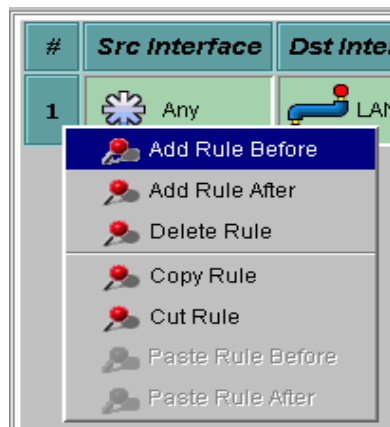
Figure 8 Header row menu



Row menu

Right-clicking on the number field in a row activates the row menu (Figure 9). This menu allows you to add a new rule at a particular location, delete the specific rule, and perform cut/copy/paste operations on a rule.

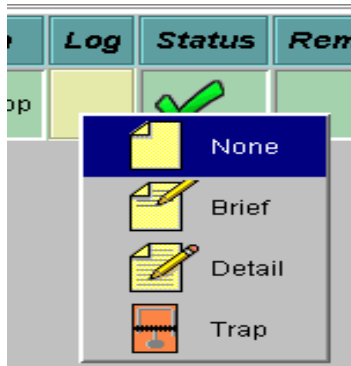
Figure 9 Row menu



Cell menus

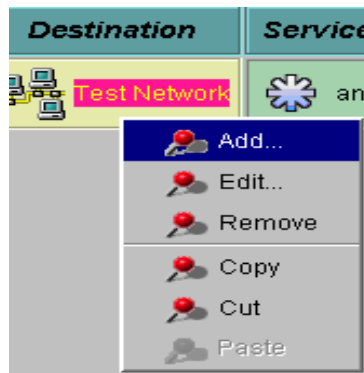
Cell menus (Figure 10) are specific to each cell and you trigger them when you right-click on an individual cell. There are two types of cell menus: option menus and procedure menus. Option menus provide a list of possible values for the cell. These menus are similar to a drop-down list box. When you click on one of the items, the selection is displayed in the cell.

Figure 10 Cell menu (option)



Procedure menus (Figure 11) provide a list of operations that you can perform on the cell, such as Add and Edit. When you click on one of the items, either the operation is performed immediately (such as Copy) or an additional dialog box appears, prompting you for more information (such as Add).

Figure 11 Cell menu (procedure)



Rule columns

Each rule within a firewall policy has the same attributes, which are specified by the column headers. All of the columns behave the same as in all three sections, except the Src Interface and the Dst Interface columns. These two columns behave differently depending on the section where the rule appears. The following sections describe the columns within a firewall rule:

#

This column specifies the ordering of the rules within the section. The order only applies to the section in which the rule appears and does not have meaning across the entire policy. If you log a rule, this number (#) is included in the log information.

Src interface and Dst interface

These columns specify the source and destination interfaces for the rule. Right-clicking on the cell displays an option menu containing possible interfaces. What appears in this option menu depends on which section of the Firewall policy the particular column appears in. For the Override and Default rules, the interfaces may only be interface groupings. These groupings are:

- Any – Any physical interface or tunnel
- Trusted – Any private physical interface or tunnel
- Untrusted – Any public physical interface
- Tunnel:Any – Any tunnel, excluding any physical interfaces

Figure 12 shows an example of a rule column.

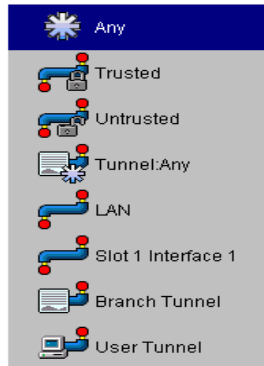
Figure 12 Rule column



For the interface-specific rules, you can specify the interfaces as either groupings or individual interfaces.

Figure 13 shows a rule column for interface-specific rules.

Figure 13 Rule column for interface-specific rules



Clicking on the user tunnel (Figure 14) or branch office (Figure 15) menu items displays the tunnel selection dialog box. This dialog box allows you to select a specific tunnel (branch office or user tunnel).

Figure 14 Tunnel dialog box for a user tunnel



Figure 15 Tunnel Selection dialog box for a branch office tunnel

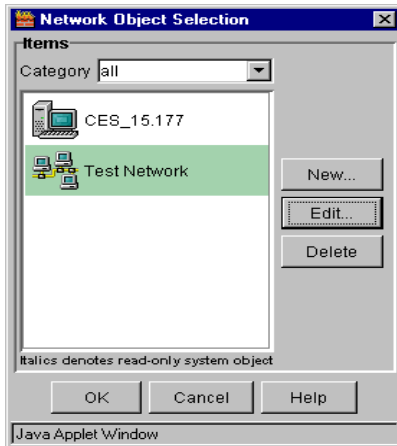
Source and Destination

These columns specify the source and destination addresses for the rule. You can modify these attributes by right-clicking on a column in the cell, which then brings up a procedure menu.

Clicking on Add displays the Network Object Selection dialog box (Figure 16). In this dialog box you define and apply a new network object. You can create the following network objects: host, network, IP range, and group (a collection of these objects).



Note: It is possible to add more than one source or destination address to a rule.

Figure 16 Network Object Selection dialog box

Italicized objects in the list are read-only and cannot be modified. The New, Edit, and Delete buttons in this dialog box allow you to create, edit and delete network objects.

Clicking on Edit displays the Network Object Edit dialog box (Figure 17). This dialog box allows you to modify the attributes for the selected network object.

Figure 17 network object edit dialog box

Clicking on Delete removes the selected network object. If the object that you want to delete is the last object, it returns to the default value.

Clicking on Copy, Cut, or Paste performs those operations on the current network object.

Service

This column specifies which services are handled by the selected rule. Right-clicking on the cell displays the standard procedure menu (Add or Edit).

Clicking on Add triggers the Service Object Selection dialog box (Figure 18), which allows you to define and apply a new service object. You can create the following service objects: tcp, udp, icmp, ip protocol, and object groups (a collection of these objects).



Note: It is possible to add more than one service to a rule.

Figure 18 Service Object Selection dialog box



Italicized objects in the list are read-only and cannot be modified. The New, Edit, and Delete buttons in this dialog box allow you to create, edit and delete network objects. Clicking on Edit displays the Service Object Edit dialog box (Figure 19). This dialog box allows you to modify the attributes for the selected service object.

Figure 19 tcp object insert dialog box

Clicking on Delete removes the selected service object from the cell. If the object to be deleted is the last object in the cell, the cell returns to its default value (in this case, Any).

Clicking on Copy, Cut, or Paste performs those operations on the current service object.

Action

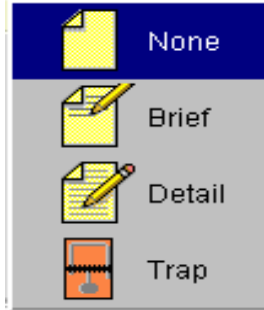
This column (Figure 20) specifies the action that occurs when the rule is activated. Right-clicking on the cell displays an option list containing three items: Accept, Drop, and Reject. Clicking on one of these items sets the cell to the selected state.

Figure 20 Action column options

Log

The Log column (Figure 21) allows you to specify the logging level for this rule. Right-clicking on this cell brings up an option list containing the following logging levels: None, Brief, Detail, and Trap.

Figure 21 Log column options



Status

This column (Figure 22) specifies the status of the particular rule. The status can be either Enabled or Disabled.

Figure 22 Status column options



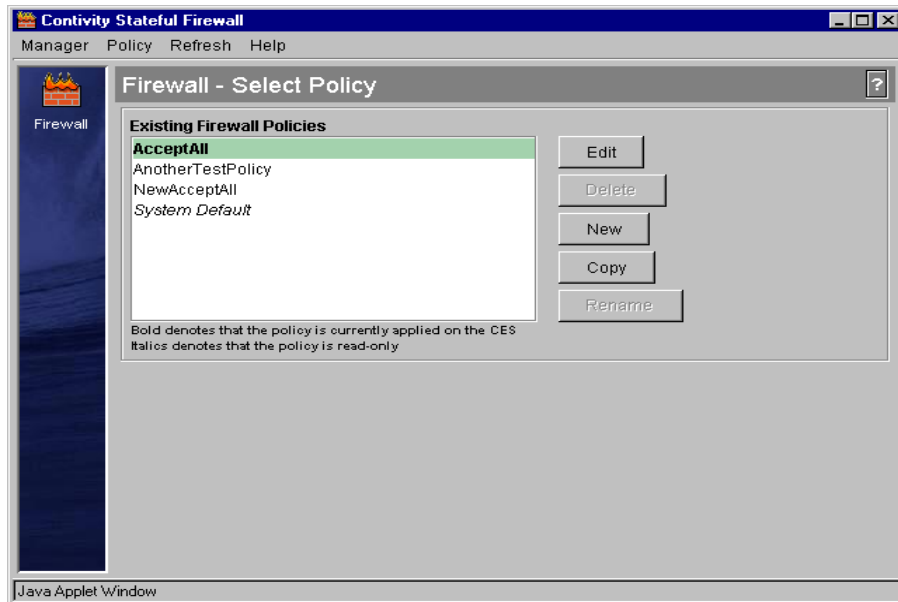
Remark

This column allows you to attach a remark to a particular rule. When you right click on Remark and choose Add or Edit remark, a dialog box appears where you can type a comment.

Creating policies

The Firewall - Select Policy screen (Figure 23) allows you to create, edit, delete, copy, or rename a firewall policy. Bold denotes the policy that is currently applied to the Contivity VPN Switch and italics denotes read-only policies. The System Default policy is always listed. This read-only policy defines the firewall behavior when no user-defined policies have been applied or when the selected policy is not available (for example, if LDAP is not available).

Figure 23 Firewall - Select Policy screen



You can add, modify or delete the rules for a policy. The screen is divided into sections that denote the rule groups. If you upgrade to a new version, the current configuration is copied to the new version. If you either upgrade or downgrade to a previous version, the configuration file and LDAP database are saved and restored.

Adding a policy

To add a new policy:

- 1 Click on the New button. The New Policy dialog box appears and prompts you for a name for the new policy.



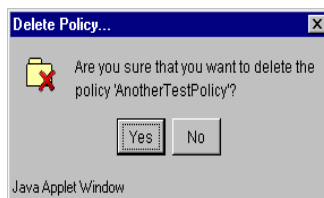
- 2 Enter the policy name. The name must begin with a letter and may not contain the : + =] , ; " characters.
- 3 Click on OK to go to the Policy Edit screen, which has a blank firewall policy, or click on Cancel to return to the policy selection screen.

Refer to the “Navigating rules” section to set up rules for your new policy.

Deleting an existing policy

You cannot delete a read-only policy or the policy that is currently applied to the switch. If you select one of these policies, the Delete button is not enabled. To delete an existing policy:

- 1 Select the policy that you want to delete and click on the Delete button. The delete policy confirmation dialog box appears.



- 2 Click on OK to delete the selected policy.

Copying an existing policy

To copy a firewall policy:

- 1 Select the policy that you want to copy.

- 2 Click on the Copy button. The copy dialog box appears.



- 3 Enter a name for the copied policy.
- 4 Click on OK.

The new policy appears in the list of policies in the firewall policies screen. This policy contains the same rules as the policy from which it was copied.

Renaming an existing policy

You cannot rename a read-only policy or the policy that is applied to the switch. If you select a read-only policy, the Rename button is not enabled. To rename an existing firewall policy:

- 1 Select the policy that you want to rename.
- 2 Click on the Rename button. The Rename dialog box appears.



- 3 Enter the new name of the policy.
- 4 Click on OK.

Creating a new policy example

Complete the following steps to configure your firewall policies.

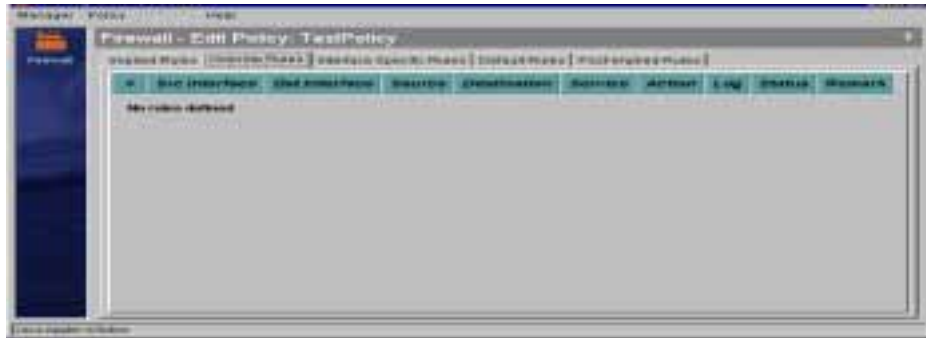
- [illegible]

-
- Linux Security Center Firewall
- Management Policy Firewall Firewall
- Firewall
- ### Firewall - Select Policy
- Selecting Firewall Policies
- iptables
 - iptables (disabled)
 - iptables (selected)**
 - System Default
- Back Cancel Next Apply Revert
- Work disabled: This policy is currently applied on the VM. Policy disabled if the policy is necessary.
- Linux Security Center

- 4** Click on **New** to create a new policy. The **New Policy** dialog box appears.

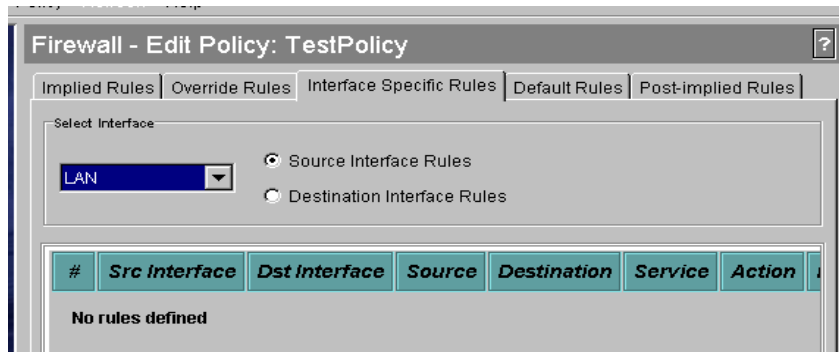


- 5 Enter the policy name and click on OK. The name must begin with a letter and may not contain the : + =] , ; " characters. The Firewall - Edit Policy: *<polycynname>* screen appears with no rules defined. In this screen, you can add, delete, and modify the rules for the policy.



- 6** You can select the rule group as follows:
 - Implied rules (view only)
 - Override rules
 - Interface-specific rules
 - Default rules
 - Post-implied rules (view only)
- 7** Select the Interface Specific Rules tab.
- 8** Select the interface from the drop-down list.

- 9 Select either Source Interface Rules or Destination Interface Rules.



- 10 Right-click on the appropriate cell to add a new rule.



- 11 Repeat these steps to add more rules.
- 12 Select Policy and click on Save Policy to save your changes.



- 13 When the policies are saved, go to the Manage menu and click on Close Manager.

Successful completion of these steps indicates that your switch's firewall is functioning and that the switch's routing patterns are available.

Verifying your configuration

When you complete the configuration tasks for the firewall, you should check the switch's routing patterns. To verify that the firewall functions properly, you can use a procedure similar to the following:

- 1** Make sure the firewall is using a security policy that allows the type of traffic you use for the test (or you can use an Accept All policy for the testing).
- 2** Verify public-to-private traffic. Perform an FTP operation from a host on the public side of the switch to a host on the private side.
- 3** Verify private-to-public traffic. Perform an FTP operation from a host on the private side of the switch to a host on the public side.
- 4** Verify tunnel-to-internal network traffic. Connect a remote Contivity VPN Switch system to the local switch. From the client, access a Web page on the internal network.
- 5** Verify tunnel-to-Internet traffic. Connect a remote Contivity VPN Client system to the switch. From the client, access a Web page on the Internet.

Chapter 3

Configuring Interface NAT

This chapter describes the steps for setting up Interface NAT.

Network Address Translation (NAT)

Network Address Translation (NAT) is the translation of one IP address that is used in the network to a different IP address that is used outside the network. This feature allows a system to be identified by one address on its own network, yet be identified by a totally different address to systems on a different network.

NAT enables private networks with private addressing to communicate with a public network (Internet) that require public addresses. Typically, companies use private addresses to increase the security of an intranet by hiding the internal IP addresses.

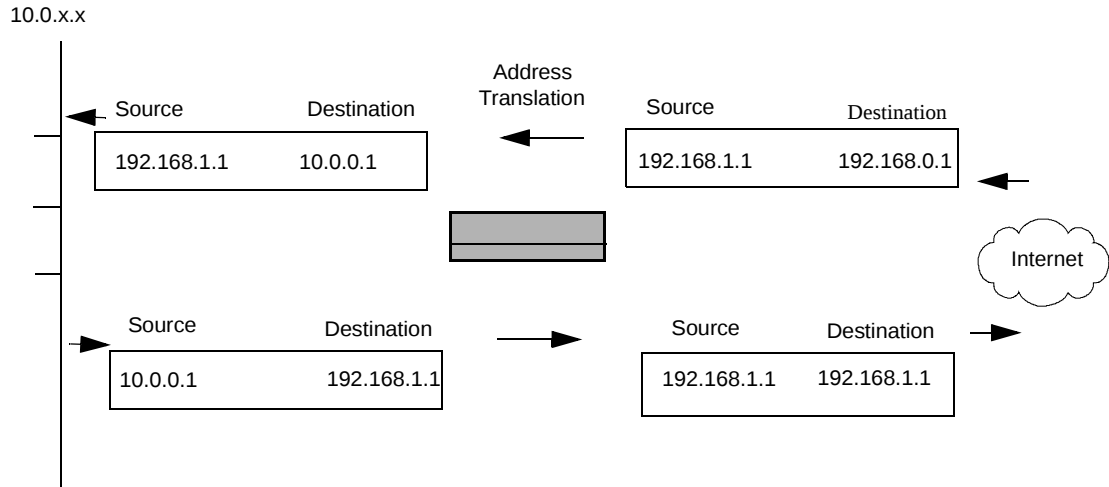
NAT allows privately addressed networks (within an intranet) to use IP addresses that are not assigned to them by the Internet Assigned Numbers Authority (IANA); for example, a *10.n.n.n* network address. NAT converts such an internal addressing scheme to an IANA-assigned address before sending a packet out to the public Internet (outside the intranet). This translation generally occurs in a network edge device such as the switch or a router.

Translation types

Static addresses map internal IP addresses to external IP addresses. This mapping does not change (unlike dynamically mapped addresses). For example, if host 10.0.0.1 is translated to 192.165.0.1 using a static rule, then an Internet host, 192.168.1.1 can initiate an FTP session using the translated external address. A host name using this rule is always bound to the same external address. For

example, 10.2.3.2 within the intranet is always translated to 192.168.34.65. A static NAT rule allows external hosts to initiate connections to internal hosts. Figure 24 shows how IP addresses are changed going from outside (Internet) to the internal network and from internal network to the Internet.

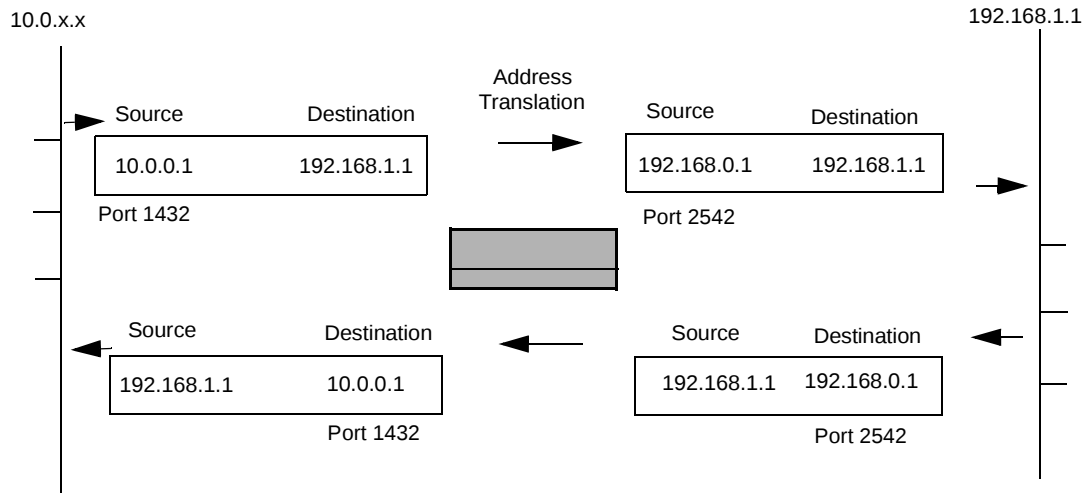
Figure 24 Static address translation



Dynamic rules include either port addressing or pooled addressing. The rules are dynamic because an address is assigned to a port or is assigned from a pool, depending on the specific situation and the conditions that currently exist for that situation. Both port and pooled addresses require external end addresses (unlike static addresses, which do not).

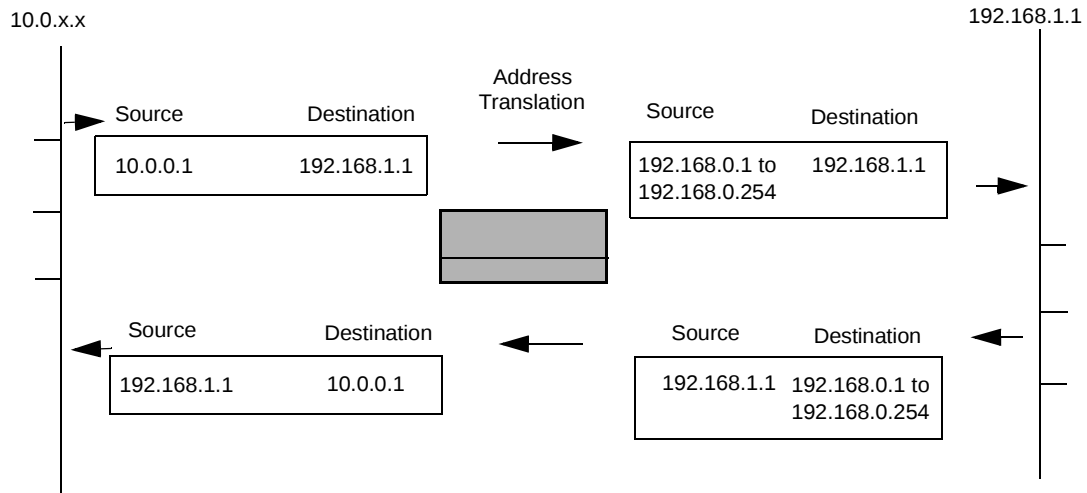
Unlike static rules, dynamic port NAT is not one-for-one. All packet transmissions must be initiated from the internal network. For dynamic port translation, the switch checks to see if the packet matches any translation table entries. If an entry exists, then it modifies the destination port and address appropriately. If there are no matching entries, the switch checks to see if the packet is initiating a connection. If so, then it allocates the next available port, adds the address and port to the translation table, and modifies the packet accordingly. It allocates the port assignment from the range of unassigned port numbers. For an incoming packet, if there are no matching entries in the translation table, it drops the packet.

Figure 25 shows how source packets from 10.0.0.1 are translated to 192.168.0.1, through port address translation for all packets from the 10.0.x.x network.

Figure 25 Port address translation

Dynamic pooled NAT is similar to dynamic port NAT. The switch checks to see if an address entry has already been allocated for this situation. If so, it updates the packet addressing and sends the packet. Otherwise, the switch attempts to allocate an address from a pool designated for this session. If an address is available, the switch adds the address pair (the original private address and the newly assigned public address) to the translation table and modifies the packet header. If there are no addresses available, it drops the packet. For an incoming packet, if there are no matching entries in the translation table, then it drops the packet.

Figure 26 shows how source packets from 10.0.0.1 are translated to an address from the pool 192.168.0.1 to 192.168.0.254, through pooled address translation for all packets from the 10.0.x.x network.

Figure 26 Pooled address translation

Interface NAT

NAT sets are collections of rules that make up a named set. You can create specific NAT sets for certain conditions, and assign the sets as they are appropriate to the conditions. NAT sets are applied to Interface NAT using the Services→Firewall screen.

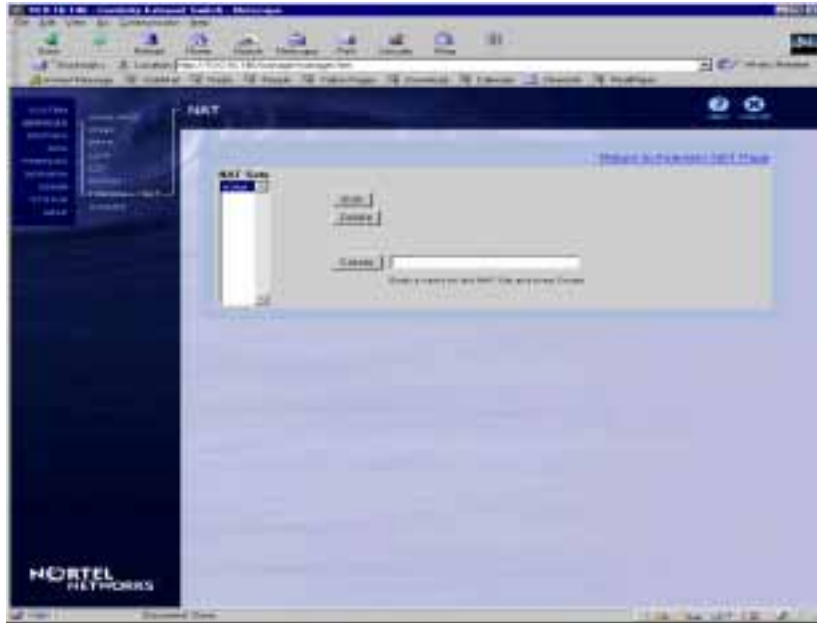
Interface NAT rules can be one of the following types:

- **Static** – for static mapping, an internal address range is mapped “one to one” to an external range.
- **Port** – for port mapping, the range of internal addresses is hidden behind a single external address. These external addresses are distinguished by using dynamically assigned port numbers.
- **Pooled** – for pooled mapping, an internal address is dynamically mapped to the next available address from the external address range.

Enabling interface NAT policies

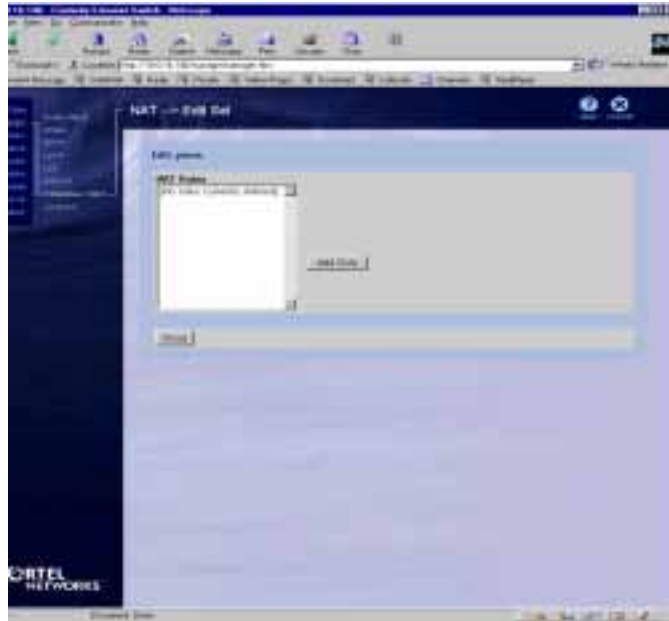
To configure a new interface NAT policy:

- 1 Go to the System→Firewall NAT screen.
- 2 Click on the Interface NAT check box under the Enabled column. The NAT Set list box shows the currently selected NAT set and lists any additional NAT sets.

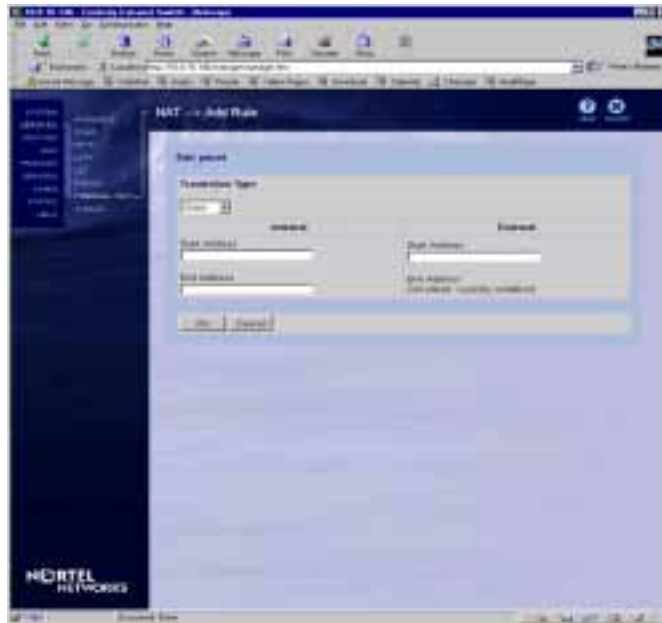


- 3 Click on the NAT Configuration link to go to the NAT Set page.

- 4 To create a new NAT set, type the name of the NAT set and click on the Create button. The NAT→Edit Set screen appears with (No rules currently defined) in the NAT Rules list box.



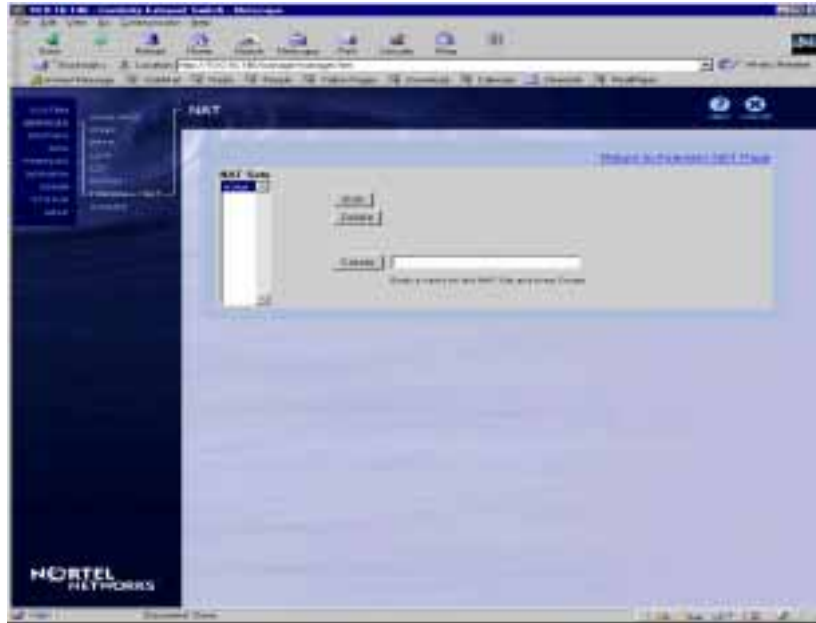
- 5 Click on the Add Rule button to add the rule. The NAT→Add Rule screen appears.



- 6 Under Translation Type, select Static, Pooled, or Port from the drop-down list.
- 7 Under Internal, enter the start (first available) and end (last available) addresses that represent the address pool that is used within the intranet.
- 8 Under External, enter the Starting External address for the address range. If the translation type is Pooled, then you must also enter an Ending External address.
- 9 Click on OK.
- 10 Click on Close to return to the NAT screen.
- 11 Click on the NAT Configuration link to go to the Profiles→NAT Sets screen to create a new NAT set if you do not want to use any of the existing ones.
- 12 You can use the Return to Firewall/NAT screen link to go back to this screen and apply the new NAT set. Selecting Interface NAT applies to non-tunneled traffic only. It does not affect the NAT sets applied to branch office tunnels. If any branch office tunnel NAT sets are assigned, they remain in effect for those branch office tunnels.

To edit an existing NAT set:

- 1 Go to the System→Firewall NAT screen.
- 2 Click on the Interface NAT check box under the Enabled column. On the NAT screen, the NAT Set list box shows the currently selected NAT set and lists any additional NAT sets.



- 3 Select the NAT set that you want to edit and click on the Edit button. The NAT→Edit Set screen appears.
- 4 Select the rule within the policy that you want to edit and click on the Edit button.

To delete a NAT set:

- 1 Go to the System→Firewall NAT screen.
- 2 Click on the Interface NAT check box under the Enabled column. The NAT Set list box shows the currently selected NAT set and lists any additional NAT sets.

- 3** Select the NAT set that you want to delete and click on the Delete button. The NAT→Delete Set screen appears, asking if you are sure you want to delete the NAT set.
- 4** Click on OK. This returns you to the NAT screen.

Chapter 4

Monitoring the Firewall

This chapter describes how to use logging and reporting on the switch to monitor the usage and tune the firewall. It also uses SNMP traps to notify you of any unusual activity. You can use a number of the same methods that you use on your switch to gain information about firewall activity. For comprehensive details on these utilities, see *Configuring the Contivity VPN Switch* or the switch's on-line help.

Logging

The Contivity Stateful Firewall logs the following events:

- Changes made to a policy in the config log
- Traffic handled by the firewall in the event log and the system log
- Detailed firewall events in the event log only

The firewall logs the following events in the config log:

- Name of any new policy created
- Name of any deleted policy
- New rules added to a policy
- Rules deleted from a policy
- Modifications to any rules

When the firewall handles traffic, the following details are written to the event log and also kept in the system log:

- Source IP and port
- Destination IP and port

- Action (allow, drop or reject)
- Rule number that was enforced

You can identify these messages by the tag CSFW.

You can control how much information is written to the system log, according to the option selected in the Log column (field) of each rule, as follows:

- None – no logging
- Brief – record only the connection information

CSFW [13] Rule[DEFAULT 5] Firewall:

[47.130.130.168:46929-201.134.251.2:135, tcp], action: Allow

- Detail – record both the connection information, plus the first 20 bytes of the IP header, and the first 20 bytes of the TCP or UDP header

CSFW [13] Rule[DEFAULT 5] Firewall:

[47.130.130.168:46929-201.134.251.2:135, tcp], action: Allow

CSFW [13] Ip Hdr: Hex[45 00 00 2c a3 78 40 00 fd 06 7c 01 2f 82 82 a8 2f f8 7c 2f]

CSFW [13] UDP/TCP Hdr: Hex[b7 51 00 87 be 04 2b be 00 00 00 00 60 02 22 38 76 01 00 00]

- Trap – same as Detail, and also trap these records

You can also send the system log records to another host using syslog. For more information, refer to *Reference for the Contivity VPN Switch*.

The following events are recorded only in the event log:

- Tunnels
- Security
- Backups
- Detailed firewall events such as conversations and flows
- Changes to hardware
- Daemon processes
- Changes to software drivers
- Interface card driver events

- Debugging messages

The event log consists of approximately 2000 records, which are kept in memory. When it is full, the oldest record is over written by the newest entry. The event log clears when you use the clear button in the GUI, or `clear` command in the CLI. The event log is written to disk only when you run the “show logging events” CLI command.

You can control how much information is written to the event log concerning the detailed firewall events. On the Firewall/NAT→Edit screen, there are six logging options:

- All – includes Traffic, Policy Manager, Firewall, and NAT
- Traffic – logs when flows and conversations are created or removed
- Policy Manager – logs firewall processes and when rules and policies are created
- Firewall – logs how the firewall handles packets within a flow
- NAT – logs NAT-related events
- Debug – creates special log messages intended for use only by Nortel Networks customer support

Firewall event logs are maintained on the switch. To view logging for the firewall, go to Status→Event Log. Firewall entries use the CSFW identifier.

To view firewall events, go to the Status→System Log (or Status→Event Log) screen or use the `show logging system` (or `show logging events`) command in the CLI.

SNMP traps

The switch supports SNMP MIB II using Gets. SNMP traps allow you to react to events that need attention or that might lead to problems. Through the community name, you can define the management stations that receive the SNMP traps. The switch supports all of the SNMP management stations including HP Open View, IBM NetView 6000, Cabletron Spectrum, and Sun Net Manager.

The switch allows the scripting of SNMP alerts so that a combination of system variables can signal an SNMP trap. When a trap occurs, the Nortel Networks icon on a standard management station turns red, signaling that there is a problem. The operator double-clicks on the icon, which then opens the browser to the Nortel Networks management interface.

The SNMP Trap Settings display (Admin→SNMP→Trap Settings) allows you to specify the level of severity that is reported for the trap. You can also specify that the trap be sent only once. The Name column lists the traps that are available for your firewall and provides status of the firewall that is currently enabled on the switch.

You can view the Health Check screen for the results of SNMP Traps.

You can also use the Health Check page to check on the current state of the Contivity Stateful Firewall. If it is running normally, the entry for the firewall is in an OK state and displays a “Contivity Stateful Firewall Active” message. If you are running the system default policy, the firewall displays a “System default policy in effect for Contivity Stateful Firewall” message. If there is an error with the current policy, the firewall entry is in an Alert state with the message “LDAP policy parse failed - using system default policy.”

Reports

The Status→Reports screen on the switch allows you to view system and performance data in text or graphical format. You can generate current or historical graphs of valuable system data. With the reports feature, you can either view a comprehensive display or download reports on firewall activity.

Clicking on Graph causes a Java applet to be loaded into your browser. When there, you can choose between graph types and time features. The first time you click Graphs, it can take a few minutes for the graphing package to download over a dial-up interface. Thereafter, it is cached and appears quickly.

Chapter 5

Command Line Interface

This chapter describes the Contivity Stateful Firewall Command Line Interface (CLI). The CLI enables you to configure the switch via a telnet or serial port session. For information on CLI commands for your switch, see *Reference for the Contivity Extranet Switch Command Line Interface*.

Accessing the CLI

Access from a telnet session

You access the CLI by starting a telnet session to the switch's management IP address, for example:

```
telnet 10.0.16.247
```

You then log in to the switch using an account with administrator privileges, for example:

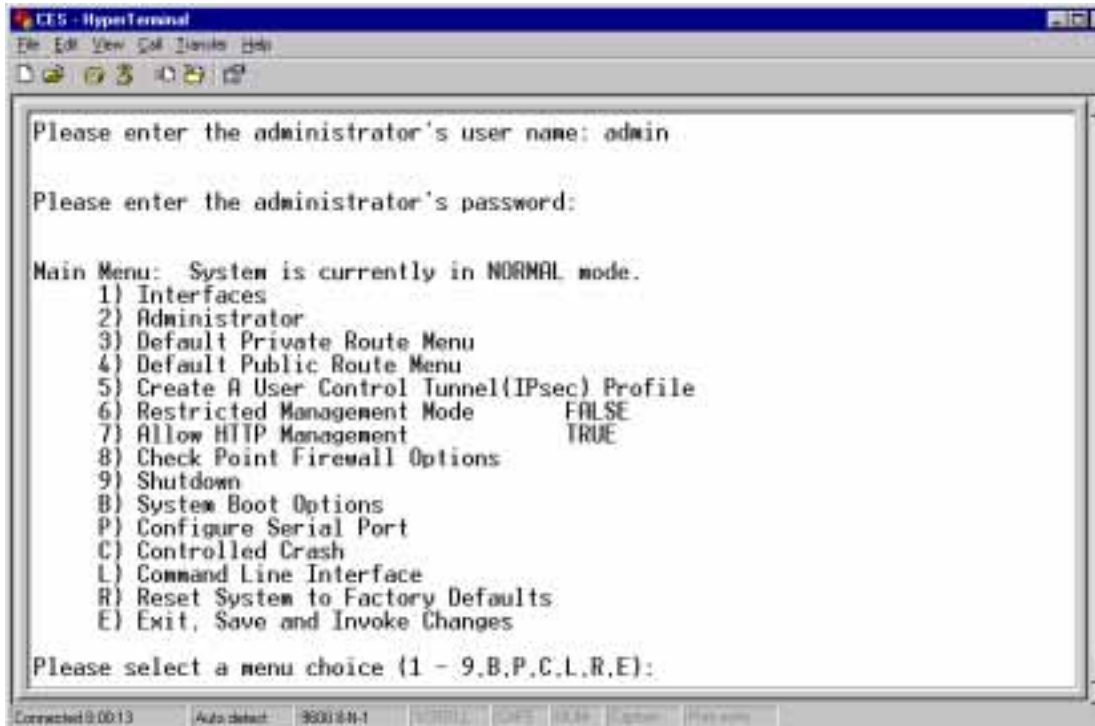
```
Login: admin
Password: *****
CES>
```

Upon login, the CLI prompt appears (CES>), indicating that you are in the CLI Exec Mode. You can execute any User Exec Mode commands or change the command mode in order to execute other commands. You can have only four telnet sessions running at one time. Each telnet session times out if idle for the amount of time set. If you change the idle time-out, it applies only to telnet sessions made after this change.

Access from the Serial Port menu

You can access the CLI through the Serial Port menu if you have a serial port connection to the switch. Select L from the Serial Port menu, shown below, to access the CLI. Figure 27 shows the Serial Port menu.

Figure 27 Serial Port menu



Command modes

The switch CLI has three command modes.

- **User Exec Mode (User Mode)**--This is the initial command mode when the administrator first establishes a telnet connection to the switch. It is also called Exec mode. You cannot modify configuration parameters or view the configuration file in this mode; however, you can clear a route.
- **Privileged Exec Mode (Priv Mode)**--This command mode is entered from User Exec mode with the `enable` command. The administrator can exit from this mode with the `disable` command and be returned to User Exec mode. Priv Mode enables more commands than in User Exec mode. Exec commands are typically one-time commands, for example, `show` commands and `clear` commands. To enter Priv mode, you must enter `enable`. If another administrator used `enable password` while in Global Config mode, the user trying to enter Priv mode must enter the correct password when prompted. To leave Priv mode and resume User mode, you can enter either `disable` or `exit`. To leave User mode and exit the telnet session or return to the Serial Port Menu, you must enter `exit`. User commands do not work in Priv mode.
- **Global Configuration Mode (Global Mode)**--This mode allows the administrator to make changes to the switch running configuration. These changes are saved across switch reboots. This mode is also used to access other configuration modes, such as LDAP, FwPolicy, and NatPolicy. The administrator enters this mode from Privileged Exec mode using the `configure terminal` command. To leave this mode and return to Privileged Exec mode, enter `exit` or `end`. For further information on CLI modes, see *Reference for the Contivity Extranet Switch Command Line Interface*.

Table 1 defines the CLI modes, their prompts, and method of access.

Table 1 CLI Modes, Prompts, and Access

Mode	Prompt	Access
User Exec Mode	CES>	Login via telnet with administrator name and password .
Privileged Exec Mode	CES#	Enter the command enable at the User Exec Mode prompt.
Global Config Mode	CES(config)#	Enter the command configure terminal at the Privileged Exec Mode prompt.
Fw Policy Mode	CES(fwpolicy)#	Enter the command policy security in Global mode.
Nat Policy Mode	CES(natpolicy)#	Enter the command policy nat in Global mode.
Ldap Mode	CES(ldap)#	Enter the command ldap server in Global mode.

The prompt reflects the current mode, the name of the device, and whether the user is privileged or not. If the user is privileged, the last character of the prompt is #. If not, the character is >. Use the **enables** or **disables** commands in the Exec mode to switch between privileged and non-privileged.

The cursor shows where typed characters will be inserted. Using the keys described in the next section, “Key bindings,” it is possible to change the location of the cursor. You can type a line that is longer than the width of the screen. If you do, the line scrolls to the left (sliding window) to allow you to type in more characters. If you move the cursor to the far left, the line scrolls to the right.

The terminal settings control the behavior of the Nortel Networks CLI (NNCLI) Parser. You can change the width of the terminal as well as the page length.

Key bindings

You can use the Nortel Networks CLI commands to edit command line text entries. Table 2 describes key bindings for NNCLI.

Table 2 Nortel Networks CLI (NNCLI) key bindings

Keys	Function
control-A	start of line
control-B	back 1 character
control-C	abort command
control-D	delete 1 character
control-E	end of line
control-F	forward 1 character
control-H &	delete character left of cursor
control-I &	command/parameter completion
control-K	delete all characters after cursor
control-L & control-R	re-display line
control-N or down arrow	next history command
control-P or up arrow	previous history command
control-Q	escape sequence for unprintables
control-T	transpose characters
control-U	delete entire line
control-W	delete word left of cursor
control-X	delete all characters before cursor delete character at cursor
control-z	“end” out of config mode
?	context-sensitive help
esc-c & esc-u	capitalize character at cursor
esc-l	convert character at cursor to lowercase
esc-b	backward 1 word
esc-d	delete 1 word to the right
esc-f	forward 1 word

Commands

firewall

This command turns the firewall on or off and specifies the firewall to use.

Syntax

```
firewall {checkpoint | contivity | policy | policy-contivity}
```

```
no firewall
```

Parameters

<i>checkpoint</i>	Enables checkpoint firewall-1.
<i>contivity</i>	Enables contivity packet filters.
<i>policy</i>	Enables contivity stateful firewall.
<i>policy-contivity</i>	Enables contivity stateful firewall and contivity packet filters.

Default

No firewall

Command mode

Global configuration

Next command mode

Global configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

The specified firewall must be available.

Warnings

% xxx firewall does not exist

Related commands

filter

policy

Example

```
CES (config) #firewall checkpoint
```

```
CES (config) #firewall contivity
```

```
CES (config) #firewall policy
```

```
CES (config) #no firewall
```

```
CES (config) #firewall policy-contivity
```

firewall anti-spoof / tunnel filter / connection number

This command turns on or off anti-spoofing or the contivity tunnel filter. It also allows you to assign a connection number for the Contivity Stateful Firewall and interface NAT.

Syntax

```
firewall {anti-spoof | tunnel-filter | connection-number number}
```

```
no firewall {anti-spoof | tunnel-filter}
```

Parameters

<code>anti-spoof</code>	Enables or disables anti-spoofing.
<code>tunnel-filter</code>	Enables or disables tunnel filters. They are always enabled when the Contivity Stateful Firewall is disabled.
<code>connection-number</code>	Specifies the number of boxes you want to connect to this switch.
<i>number</i>	This number is the connection number, which has a minimum and maximum number for different switches. This number cannot be beyond the min-max connection number range.

Default

Anti-spoofing defaults are disabled.

Tunnel-filter defaults are enabled (always enabled when Contivity Stateful Firewall is disabled).

The default connection number is different for each switch and each has minimum and maximum connection numbers.

Command mode

Global configuration

Next command mode

Global configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

% Invalid connection number

% Connection number has to be between xxx and xxx on this switch!

Related commands

filter

policy

Example

```
CES (config) #firewall anti-spoof
CES (config) #firewall tunnel-filter
CES (config) #firewall connection-number 1000
CES (config) #no firewall anti-spoof
CES (config) #no firewall tunnel-filter
```

firewall logging

This command turns on or off different types of firewall-related logs that display different event logs.

Syntax

```
firewall logging {all | traffic | polmgr | firewall | nat | debug}
```

```
no firewall logging {all | traffic | polmgr | firewall | nat |  
debug}
```

Parameters

<i>all</i>	Enables or disables all traffic, policy manager, firewall and NAT logging.
<i>traffic</i>	Enables or disables traffic logging.
<i>polmgr</i>	Enables or disables policy manager logging.
<i>firewall</i>	Enables or disables firewall logging.
<i>nat</i>	Enables or disables NAT logging.
<i>debug</i>	Enables or disables debug logging.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

The specified firewall must be available.

Example

```
CES (config) #firewall logging traffic
CES (config) #firewall logging polymgr
CES (config) #firewall logging firewall
CES (config) #firewall logging nat
CES (config) #firewall logging all
CES (config) #firewall logging debug
```

license

This command enables or disables paid feature license keys.

Syntax

```
license install license-key
```

```
no license license-key-prefix
```

Parameters

license-key Represents a valid paid feature license key. The first two characters of this key represent the license key prefix. Valid prefixes are `fw` (for firewall) and `ar` (for advanced routing).

license-key-prefix Two character string that specifies which license key is removed. Valid *license-key-prefixes* are `fw` (for firewall) and `ar` (for advanced routing).

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

% Failed to remove paid feature feature-name

% Unknown paid feature feature-name

% Invalid license key

Related commands

`show license`

Example

```
CES (config-natpolicy) #license install fw-7384034-0342859268-d4
```

```
CES (config-natpolicy) #no license fw
```

Comments

None

netobj

This command adds, edits, or deletes the specific network object or netobj group for the user scope in the policy based firewall. Net objects of master scope are created dynamically and you cannot edit or delete them.

Syntax

```
netobj [add] name {host {ip-address} |  
network {network-address} |  
ip-range {ip-address1 ip-address2} | group}  
  
no netobj name
```

Parameters

add	Creates a new net object or group for the user scope, which can be assigned to policy rules.
<i>name</i>	Name of net object or group for firewall policy to edit. You cannot create a name if it already exists.
host	A network host that is specified by the IP address.
<i>network-address</i>	The network address to be assigned to the specific network object such as host, network. This is of the form <i>ip-address/ip-mask</i> .
network	A network specified by an IP address and a mask.
ip-range	A range of IP addresses with a format similar to <i>IP-addresss1 IP-address2</i> .
group	Creates a new netobj group with the specific name. It only works with keyword add.

Default

None

Command mode

Firewall policy configuration

Next command mode

Firewall policy configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

% Netobj xxx does not exist (when editing)

% Netobj xxx already exists (when adding)

Related commands

netobj-group

service

Example

```
CES (config-fwpolicy) #netobj test1 host 10.0.10.123
```

```
CES (config-fwpolicy) #netobj add test2 ip-range 10.0.0.1 10.0.0.50
```

```
CES (config-fwpolicy) #netobj test3 network 10.23.0.0 255.255.0.0
```

```
CES (config-fwpolicy) #netobj testgroup group
```

```
CES (config-fwpolicy) #no netobj test4
```

netobj-group

This command adds, edits, or deletes the specific network object group for the user scope in the Contivity Stateful Firewall. Net object groups of master scope are created dynamically and you cannot edit or delete them.

Syntax

`netobj-group netobj-group-name { add | drop } netobj-names`

Parameters

netobj-group-name Name of netobj group for firewall policy to edit.

add Adds netobjs to the specific group. Netobj groups of master scope are created dynamically and cannot be edited.

drop Removes netobjs from specific group. Netobj groups of master scope are created dynamically and cannot be edited.

netobj-names Names of the netobjs. Can be one or more.

Default

None

Command mode

Firewall policy configuration

Next command mode

Firewall policy configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

% Netobj xxx is read-only

% Netobj xxx does not exist

% Netobj xxx is not a group

% Netobj xxx already exists in group yyy (when adding a netobj)

% Netobj xxx does not exist in group yyy (when dropping a netobj from a group)

Related commands

netobj

service group

Example

```
CES (config-fwpolicy) #netobj-group testgroup add test1 test2
```

```
CES (config-fwpolicy) #netobj-group testgroup drop test1
```

policy nat

This command creates a specified NAT set for the switch and puts the CLI into NAT configuration mode.

Syntax

```
policy nat [add] natname
```

```
no policy nat natname
```

Parameters

add	Creates a new NAT set for the switch.
<i>natname</i>	Name of NAT set to edit or add.

Default

None

Command mode

Global configuration

Next command mode

Nat policy configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

% NAT set xxx does not exist (when editing or deleting).

% NAT set xxx already exists (when adding).

Related commands

policy

Example

```
CES (config) #policy nat add testnat
```

```
CES (config) #policy nat testnat
```

```
CES (config-natpolicy) #exit
```

```
CES (config) #no policy nat testnat
```

policy nat interface

This command turns on or off interface NAT and specifies the type of NAT policy to use.

Syntax

```
policy nat interface [enable | disable | assign natname]
```

Parameters

<code>enable</code>	Turns on interface NAT.
<code>disable</code>	Turns off interface NAT.
<code>assign</code>	Specifies a NAT set for interface NAT.
<i>natname</i>	Name of NAT set to assign.

Default

None

Command mode

Global configuration

Next command mode

Global configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

% NAT set xxx does not exist!

% Interface NAT is already enabled!

% Interface NAT is already disabled!

Related commands

policy security

policy nat

Example

```
CES (config) #policy nat interface enable
```

```
CES (config) #policy nat interface disable
```

```
CES (config) #policy nat assign mynatset
```

policy security

This command puts you in firewall policy configuration mode for the given policy name. If you specify the optional **add** parameter, the command creates the specified policy and enters firewall policy configuration mode. If the optional **assign** parameter is specified, the command assigns a specific policy to the switch and remains in global configuration mode. If you specify neither **add** or **assign**, the command enters firewall policy configuration mode and opens the specified policy for editing. The **no** form of this command deletes the specified policy from the switch.

Syntax

```
policy security [{add |assign}] policy-name
```

```
no policy security policy-name
```

Parameters

security	Settings for the security policy.
add	Creates a new policy for the policy-based firewall, then puts the CLI into firewall policy configuration mode.
assign	Specifies one policy to be used for the current firewall.
<i>policy-name</i>	Name of policy for the policy-based firewall to edit.

Default

None

Command mode

Global configuration

Next command mode

Firewall policy configuration for adding and editing
Global configuration for assigning

Required privileges

System Management - Manage

User Management - None

Prerequisites

Policy-based firewall must be available on the switch.

Warnings

% Policy xxx does not exist (when editing or deleting or assigning)

% Policy xxx already exists (when adding)

% Policy xxx is in use and can not be deleted

Related commands

firewall
filter
policy nat

Example

```
CES (config) #policy security add test1
CES (config-fwpolicy) #exit
CES (config) #policy security assign test2
CES (config) #policy security test3
CES (config-fwpolicy) #exit
CES (config) #no policy security test4
```

rule (Firewall Policy Configuration)

This command adds or edits the specified firewall policy rule to the current firewall policy in the Contivity Stateful Firewall. When you add a rule, the firewall always adds the rule to the top of the rule group. You cannot use the CLI to reorder rules within a group; you must cut and paste them in the order you want to use. For further information on the rule parameters, see Chapter 2, “Configuring the Firewall.”

Syntax

```
rule {default | override | {interface interface-name {source |  
destination}} {add | rule-number} [src-interface interface-name]  
[dest-interface interface-name] [src-address address] [dest-address  
address] [service service-name] [action action-name] [log  
log-level] [remark text]
```

```
no rule {default | override | {interface interface-name {source |  
destination}} number
```

Parameters

default	Specifies that the rule is a default rule.
override	Specifies that the rule is an override rule.
interface	Specifies that the rule is an interface rule.
source	Specifies that the interface rule is a source interface rule.
destination	Specifies that the interface rule is a destination interface rule.
add	Specifies that the policy rule should be created.
<i>rule-number</i>	Rule number in this firewall policy rule set.
src-interface	Settings are for the source interface. Not recognized for source interface rules.
dest-interface	Settings are for the destination interface. Not recognized for destination interface rules.
<i>interface-name</i>	The interface-name for override rules can be trusted, untrusted, any or tunnel:any. For a source interface rule, the interface-name of destination interface can be any, an end user interface (T0 - Tn), a branch office interface (Tx, - Ty), a physical interface (E0 - En), trusted, untrusted, tunnel:any or system-ip. For a destination interface rule, the interface-name of source interface can be any, trusted, untrusted, tunnel:any.
src-address	Settings are for the source address.
dest-address	Settings are for the destination address.

<i>address</i>	IP address for the source or destination. Can be a dotted IP address, a host name, an IP address and mask which specifies a subnet, or any.
<i>service</i>	Set the service for the current firewall policy rule.
<i>service-name</i>	Name of the service. Can be any or a predefined protocols such as FTP, HTTP, Telnet, SMTP, etc. It can also be a protocol (TCP or UDP) followed by a port number.
<i>action</i>	Set the action for the current firewall policy rule.
<i>action-name</i>	Name of the action. Can be accept, drop or reject.
<i>log</i>	Event log.
<i>log-level</i>	Can be one of none, brief, detail, trap. Trap is the same as detail, but also enables SNMP traps on a rule match.
<i>remark</i>	The comments users can put in.
<i>text</i>	The content of the remark. If the value for the text parameter contains spaces, it may be enclosed in double quotes so that it has a single parameter value.

Default

For newly created rules, the default action is reject. The firewall determines the default interface by the type of rule group to which it belongs. In interface rule set, either source interface or destination interface has a default value that you cannot change. The default settings of other fields are Any.

Command mode

Firewall policy configuration

Next command mode

Firewall policy configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

None

Warnings

- % Rule xxx does not exist
- % Invalid interface name
- % Invalid network address
- % Invalid service name
- % Invalid number of arguments

Related commands

policy

Example

```
CES (config-policy) #rule override 3 src-interface untrusted
src-address 192.32.0.0 dst-address 192.32.240.11 service ftp action
accept log full remark "This is for test"
```

```
CES (config-policy) #rule interface "Tunnel:/Base/myTunnel" source
add dst-address 192.32.240.11 service ftp action accept log full
remark "This is for test"
```

```
CES (config-policy) #rule interface "Tunnel:/Base/myTunnel" source
3 dst-address 192.32.240.12 service ftp action accept log brief
```

```
CES (config-policy) #rule default 3 src-address 192.32.0.0 service
ftp action accept
```

```
CES (config-policy) #no rule interface "Tunnel:/Base/myTunnel" 3
```

```
CES (config-policy) #no rule override 3
```


rule (NAT Policy Configuration)

This command edits or adds the specified NAT rule to the current NAT set.

Syntax

```
rule [add] rule-number {static internal start-address end-address
external start-address | pooled internal start-address end-address
external start-address end-address | port internal start-address
end-address external start-address}
```

```
no rule rule-name
```

Parameters

add	Specifies that the NAT rule should be created.
<i>rule-number</i>	Number of the NAT rule. This number appears when you use the <code>show rules all</code> command, which displays the list of NAT rules indexed by numbers.
static	Static address translation rules
internal	Addresses are used within the intranet.
<i>start-address</i>	First available address that is used within the intranet address pool or used for the public network.
<i>end-address</i>	The last available address that is used within the intranet address pool or used for the public network.
external	Addresses are used for the public network (Internet).
pooled	Settings are for the dynamic pooled NAT.
port	Settings are for the dynamic port NAT.

Default

None

Command mode

NAT policy configuration

Next command mode

NAT policy configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

% Invalid address

% NAT rule xxx does not exist (when editing or deleting)

% NAT rule xxx already exists (when adding)

Related commands

nat

Example

```
CES (config-nat) #rule testrule1 static internal 10.0.10.111
10.0.10.200 external 202.96.3.44
```

```
CES (config-nat) #rule add testrule2 pooled internal 10.0.10.111
10.0.10.200 external 202.96.3.0 202.96.3.255
```

```
CES (config-nat) #rule testrule3 port internal 10.0.10.111
10.0.10.200 external 202.96.3.44
```

```
CES (config-nat) #no rule testrule
```

service

This command adds, edits, or deletes the specific service or service group for the user scope in the policy-based firewall. Services of master scope are created dynamically and you cannot edit or delete them.

Syntax

```
service [add] name
{tcp {port-num num | port-range num1 num2} |
udp {port-num num | port-range num1 num2} |
ip protocol-num num |
icmp {type-num num | any} |
      code-num num | any} |
      code-range num1 num2
|}
group}

no service name
```

Parameters

add	Creates a new service or group that can be assigned to policy rules.
<i>name</i>	Name of service or service group for firewall policy to edit. You cannot create any name that already exists.
tcp	Service type TCP.
udp	Service type UDP.
ip	Service type IP.
icmp	Service type ICMP.
port-num	Number of port.
protocol-num	Number of protocol.
type-num	ICMP type number.
code-num	ICMP code number.
<i>num</i>	Number used for tcp/udp port-num, tcp/udp port-range, ip protocol-num, icmp type-num, icmp code-num, icmp code-range.
code-range	Range of ICMP code numbers.
group	Creates a new service group with the specific name. It only works with key word add.

Default

None

Command mode

Firewall policy configuration

Next command mode

Firewall policy configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

% Service xxx does not exist (when editing or deleting)

% Service xxx already exists (when adding)

Related commands

service-group

netob

Example

```
CES (config-fwpolicy) #service add test1 tcp 111
CES (config-fwpolicy) #service add test2 icmp type 23 code 45
CES (config-fwpolicy) #service add test3 udp 23 45
CES (config-fwpolicy) #service add test4 ip 10
CES (config-fwpolicy) #service add testgroup1 group
CES (config-fwpolicy) #service test2 icmp type 23 code 45 50
CES (config-fwpolicy) #no service test3
```

service-group

This command adds, edits, or deletes the specific service group in the Contivity Stateful Firewall. Service groups of master scope are created dynamically and you cannot edit or delete them.

Syntax

```
service-group service-group-name {add | drop} service-names
```

Parameters

<i>service-group-name</i>	Name of service group for which you can edit firewall policy.
add	Adds services to the specific group. Service groups of master scope are created dynamically and cannot be edited.
drop	Removes services from specific group. Service groups of master scope are created dynamically and cannot be edited.
<i>service-names</i>	Names of the services. Can be one or more.

Default

None

Command mode

Firewall policy configuration

Next command mode

Firewall policy configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

% Service xxx is read-only

% Service xxx does not exist

% Service xxx is not a group

% Service xxx already exists in group yyy (when adding a service to a group)

% Service xxx does not exist in group yyy (when dropping a service from a group)

Related commands

netobj-group

service

Example

```
CES (config-fwpolicy) #service-group testgroup1 add test1 test2
```

```
CES (config-fwpolicy) #service-group testgroup1 drop test1
```

show firewall

This command displays all available firewall types or the firewall that is currently in use. It can also display firewall logging information.

Syntax

```
show firewall {all | enabled | logging | anti-spoof | tunnel-filter
| connection-number}
```

Parameters

all	Displays all available firewall types, which include Check Point Firewall, Policy-based Firewall, Contivity Stateful Firewall, or Policy and Contivity Stateful Firewall, which co-exist.
enabled	Displays the firewall type that is turned on, if any.
logging	Displays the firewall logging types (traffic, policy manager, firewall, NAT or debug) that are disabled or enabled.
anti-spoof	Displays the enabled or disabled status of anti-spoofing.
tunnel-filter	Displays the enabled or disabled status of the tunnel filters.
connection-number	Displays the currently specified connection number and the minimum/maximum number on this switch.

Default

None

Command mode

Global configuration

Next command mode

Global configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

None

Warnings

None

Related commands

policy security

Example

```
CES (config) #show firewall all
CES (config) #show firewall enabled
CES (config) #show firewall logging
CES (config) #show firewall anti-spoof
CES (config) #show firewall tunnel-filter
CES (config) #show firewall connection-number
```


show interfaces

This command displays the available interfaces that you can apply to a policy or a policy rule.

Syntax

```
show interfaces [ tunnel | bo-tunnel | | physical | all ]
```

Parameters

tunnel	Displays a list of tunnel interface which are available on the switch.
bo - tunnel	Displays a list of branch office tunnel interface which are available on the switch.
physical	Displays all of the available physical interfaces on the switch.
all	Displays all of the available interfaces on the switch.

Default

None

Command mode

Firewall policy configuration

Next command mode

Firewall policy configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

None

Related commands

show netobjs

show services

Example

```
CES (config-fwpolicy) #show interfaces
```

```
CES (config-fwpolicy) #show interfaces all
```

```
CES (config-fwpolicy) #show interfaces tunnel
```

```
CES (config-fwpolicy) #show interfaces bo-tunnel
```

show license

This command displays the status of paid features on the CES.

Syntax

```
show license
```

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

None

Related commands

license
no license

Example

```
CES (config-natpolicy) #show license
Advanced Routing: Enabled
Contivity Stateful Firewall: Enabled
```

Comments

None

show netobjs

This command displays all of the available netobjs and netobj groups that you can use for firewall policies.

Syntax

```
show netobjs [netobj-type]
```

Parameters

netobj-type Restricts display of netobjs to specified type. Valid types are host, network, ip_range, and group.

Default

None

Command mode

Firewall policy configuration

Next command mode

Firewall policy configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

None

Related commands

show netobjs

Example

```
CES (config-fwpolicy) #show netobjs
CES (config-fwpolicy) #show netobjs host
CES (config-fwpolicy) #show netobjs network
CES (config-fwpolicy) #show netobjs ip_range
```

show policy nat

This command displays all available NAT sets on the switch. If you specify keyword interface, it displays interface NAT information.

Syntax

```
show policy nat [interface]
```

Parameters

nat	Displays a list of NAT sets that are available on the switch.
interface	Displays the status of interface NAT (on or off) and the NAT set assigned to it.

Default

None

Command mode

Global configuration

Next command mode

Global configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

None

Warnings

None

Related commands

show policy
show firewall

Example

```
CES (config) #show policy nat  
CES (config) #show policy nat interface
```


show policy security

This command displays all of the available firewall policies or the policy currently in use.

Syntax

```
show policy security {all | enabled}
```

Parameters

security	Specifies firewall policies.
all	Displays the names of all of the available policies.
enabled	Displays the policy that is currently in use.

Default

None

Command mode

Global configuration

Next command mode

Global configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

none

Related commands

show firewall

Example

```
CES(config)#show policy security all
```

```
CES(config)#show policy security enabled
```

show rules (Firewall Policy Configuration)

This command displays all of the available rules for the current override, interface, or default rule mode. The displayed rules are ordered by number.

Syntax

```
show rules {default | override | interface interface-name}
```

Parameters

<code>all</code>	Displays all of the rules in the policy.
<code>implied</code>	Displays read-only implied rules.
<code>post-implied</code>	Displays read-only post-implied rules.
<code>default</code>	Displays all rules in the default rule set.
<code>override</code>	Displays all rules in the override rule set.
<code>interface</code>	Displays the rules in the interface rule set with either a source or destination interface of <i>interface-name</i> .
<i>interface-name</i>	Specifies the name of the interface to display rules for in the interface rule set.

Default

None

Command mode

Firewall policy configuration

Next command mode

Firewall policy configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

None

Related commands

show policy

Example

```
CES (config-fwpolicy) #show rules default
CES (config-fwpolicy) #show rules override
CES (config-fwpolicy) #show rules interface LAN
CES (config-fwpolicy) #show rules all
CES (config-fwpolicy) #show rules implied
CES (config-fwpolicy) #show rules post-implied
```

show rules (NAT Policy Configuration)

This command displays available NAT rules.

Syntax

```
show rules {all | rule-number}
```

Parameters

<i>all</i>	Displays all of the NAT rules that are available in the switch.
<i>rule-number</i>	Displays the NAT rule with the specific number. This number appears when you use the <code>show rules all</code> command, which displays the list of NAT rules indexed by numbers.

Default

None

Command mode

NAT policy configuration

Next command mode

NAT policy configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

None

Warnings

% NAT rule xxx does not exist.

Related commands

show policy

Example

```
CES (config-natpolicy) #show rules all
CES (config-natpolicy) #show rules 2
```

show services

This command displays all of the available services and service groups you can use for firewall policies in the Contivity Stateful Firewall.

Syntax

```
show services [service-type]
```

Parameters

service-type Restricts display to show only services of specified type. Valid types are *TCP*, *UDP*, *ICMP*, *IP*, and *group*.

Default

None

Command mode

Firewall policy configuration

Next command mode

Firewall policy configuration

Required privileges

System Management - Manage

User Management - None

Prerequisites

None

Warnings

None

Related commands

show netobjs

Example

```
CES (config-fwpolicy) #show services
CES (config-fwpolicy) #show services ip
CES (config-fwpolicy) #show services tcp
```

Appendix A

Error Messages

This appendix provides a listing of possible syslog messages that the Contivity Stateful Firewall might write to a remote system. Each message is followed by a description and the recommended corrective action, if any.

Firewall messages

An error occurred while parsing the policy

Description: The policy that you are attempting to view or edit cannot be opened because it does not conform to the required format. This may be caused by an error in the LDAP database or a problem with the connection to the switch.

Action:

- 1** Close the Contivity Stateful Firewall Manager.
- 2** Close all instances of the browser used to load the Contivity Stateful Firewall Manager.
- 3** Be sure that the connection to the switch is established.
- 4** Be sure that the LDAP server containing the policy is properly configured and is active.
- 5** Restart the browser and navigate to the System→Firewall screen.
- 6** Reload the Contivity Stateful Firewall Manager.

An error occurred while communicating with the switch

Description: The Contivity Stateful Firewall Manager encountered an error while retrieving the data from the switch. This may have been caused by a network error or the switch may have stopped responding.

Action:

- 1** Close the Contivity Stateful Firewall Manager.
- 2** Close all instances of the browser used to load the Contivity Stateful Firewall Manager.
- 3** Be sure that the connection to the switch is established.
- 4** Restart the browser and navigate to the System→Firewall screen.
- 5** Reload the Contivity Stateful Firewall Manager.

Authorization failed. Please try again.

Description: This error occurs when the wrong authentication credentials are entered. The user is re-prompted for credentials until they are either correct or the user clicks Cancel.

Action: No action required.

Unable to communicate with the switch

Description: The Contivity Stateful Firewall Manager cannot establish a connection to the switch. This may have been caused by a network error or the switch may not be responding to requests.

Action:

- 1** Close the Contivity Stateful Firewall Manager.
- 2** Close all instances of the browser used to load the Contivity Stateful Firewall Manager.
- 3** Be sure that the connection to the switch is established.
- 4** Restart the browser and navigate to the System→Firewall screen.

5 Reload the Contivity Stateful Firewall Manager.

The contents of the database may have changed...

Description: This error occurred because the LDAP database has changed in such a way that the current data in the Contivity Stateful Firewall Manager might not be valid. This error is encountered when the:

- Internal LDAP server has been shut down and restarted
- External LDAP server in use is switched to the internal LDAP server
- Internal LDAP server in use is switched to an external LDAP server
- External LDAP server's port or IP address changes

Action:

To ensure that the most current data is loaded:

- 1 Close the current policy, if opened. Saving is not permitted until this error is remedied.
- 2 From the policy selection screen, select All from the Refresh menu.

System files were not loaded properly ...

Description: This error occurred because the files necessary to load the Contivity Stateful Firewall Manager were either not downloaded from the switch properly or were not initialized properly.

Action:

If this error is encountered:

- 1 Close the Contivity Stateful Firewall Manager.
- 2 Close all instances of the browser used to load the Contivity Stateful Firewall Manager.
- 3 Restart the browser and navigate to the System→Firewall screen.
- 4 Reload the Contivity Stateful Firewall Manager.

If the error continues to occur or if the Contivity Stateful Firewall Manager is being accessed through a user tunnel:

- 1** Open the Java Plug-in Properties.
- 2** On Windows systems, navigate to Start→Settings→Control Panel→Java Plug-in. For all other systems, refer to the Java Plug-in documentation.
- 3** Be sure that the check box for Cache JARs in Memory is deselected.
- 4** Click on Apply and close the Java Plug-in Properties window.
- 5** Close the Contivity Stateful Firewall Manager.
- 6** Close all instances of the browser used to load the Contivity Stateful Firewall Manager.
- 7** Restart the browser and navigate to the System→Firewall screen.
- 8** Reload the Contivity Stateful Firewall Manager.

Index

A

actions on rules 47
administrator privileges 71
anti-spoofing 21
attack detection 21

C

cell menu 41
columns
 Dst interface 42
 Src interface 42
components 18
configuration
 firewall 51
 initial 29
 verifying 55
conversation 19

D

default rules 38

E

error messages 121

F

filtering 20
firewall
 components 18
 configuring 51
 installation prerequisites 24

 options 21, 32
firewall anti-spoof command 78
firewall command 76
firewall connection number command 78
firewall logging command 80
firewall tunnel filter command 78

G

graphs 70

H

header row menu 40

I

implied rules 35, 39
installation prerequisites 24
interface NAT 57
interfaces 19
interface-specific rules 36

J

Java 2
 Netscape 26
Java 2 Runtime Environment
 Internet Explorer 25
 Netscape 6 28
 Netscape on Solaris 28

L

licence
 command 82
license 23
log column 48
logs 67
 levels 48

M

Management IP Address 71
menus
 cell 41
 header row 40
 row 40

N

NAT
 configure new policy 64
 dynamic 58
 dynamic pooled 59
 dynamic port 58
 editing existing set 64
 rules 20
netobj command 84
netobj-group command 86
Network Address Translation (NAT) 57
network objects 44

O

override rules 36

P

policies
 actions 33
 adding 49
 components 32
 copying 50
 creating 33, 49

 deleting 50
 editing 33
 renaming 51
 selecting 49
policy command 92
policy nat command 88
policy nat interface command 90
pooled translation type 60
post-implied rules 35, 39

R

remarks 48
reports 70
row menu 40
rule (Firewall Policy Configuration) command 94
rule (NAT Policy Configuration) command 97
rule column 42
rules
 default 38
 implied and post-implied 35, 39
 in policies 19
 interface-specific 36
 navigating 34, 39
 override 36

S

serial Port 72
service command 99
service objects 46
service-group command 101
show firewall command 103
show interfaces command 105
show license command 107
show netobjs command 109
show policy command 113
show policy nat command 111

- show rule (NAT Policy Configuration)
 - command 117
- show rules (Firewall Policy configuration)
 - command 115
- show services command 119
- SNMP
 - MIB II 69
 - overview 69
 - traps 69
- stateful inspection 18
 - application 18
 - TCP 18
- static
 - translation type 60
- static address NAT 57
- static translation type 60
- status 48
- system messages
 - certificate 121
- system requirements 24

T

- Telnet 71

